Securing Network Layers

Information Assurance

Lesson Objectives

- Students will learn about Virtual Private Networks (VPN) and IP Security (IPSec); to include the authentication and encapsulating security payload modes and the transport and tunnel modes. Security association and IPSec key distribution schemes will also be covered.
- Students will also learn about host-to-host security protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS), Pretty Good Privacy (PGP), S/MIME. Commercial based security devices such as firewalls and intrusion detection systems will be covered in detail.

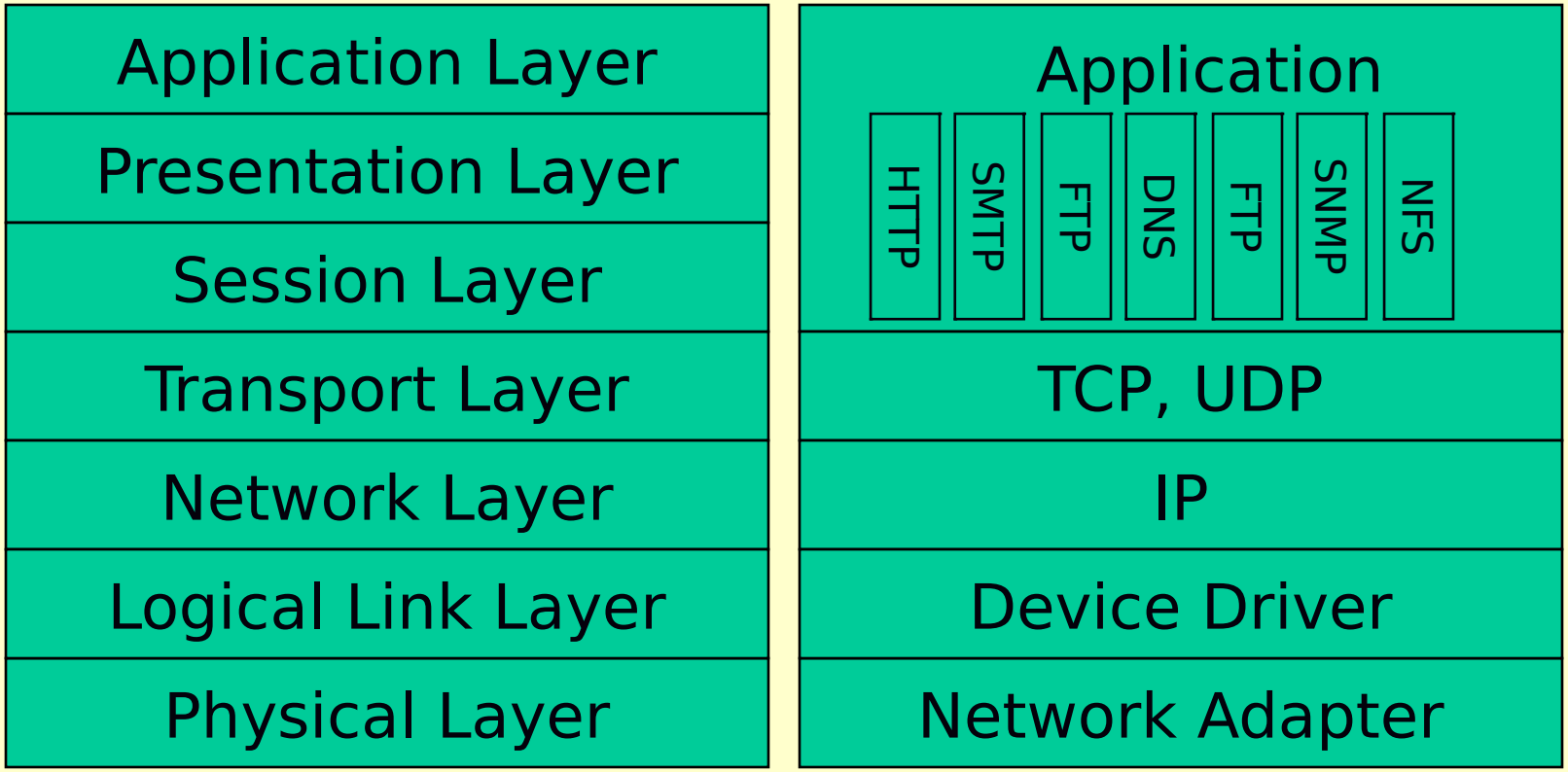
Securing Network Layers Outline

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

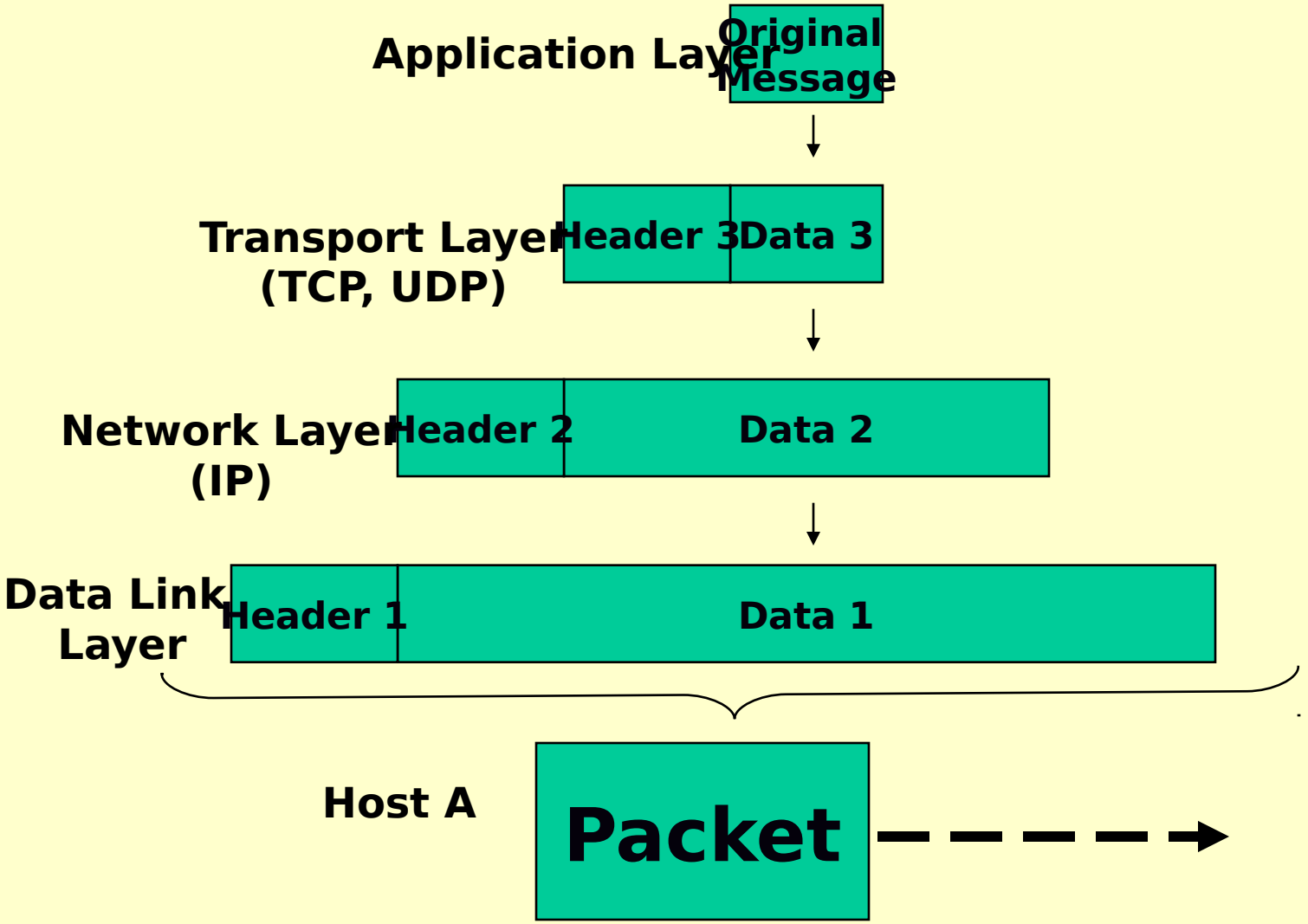
Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

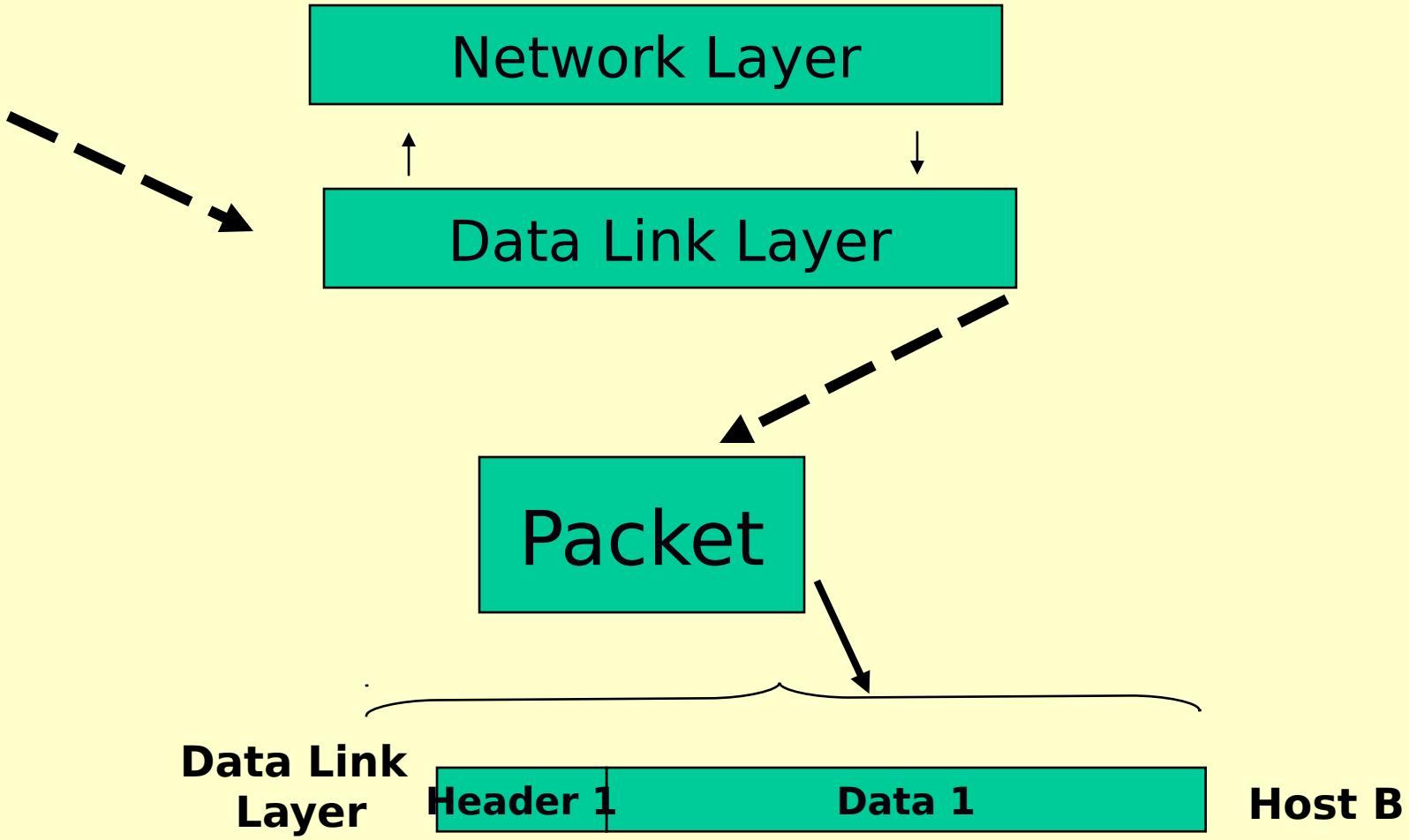
TCP/IP Review



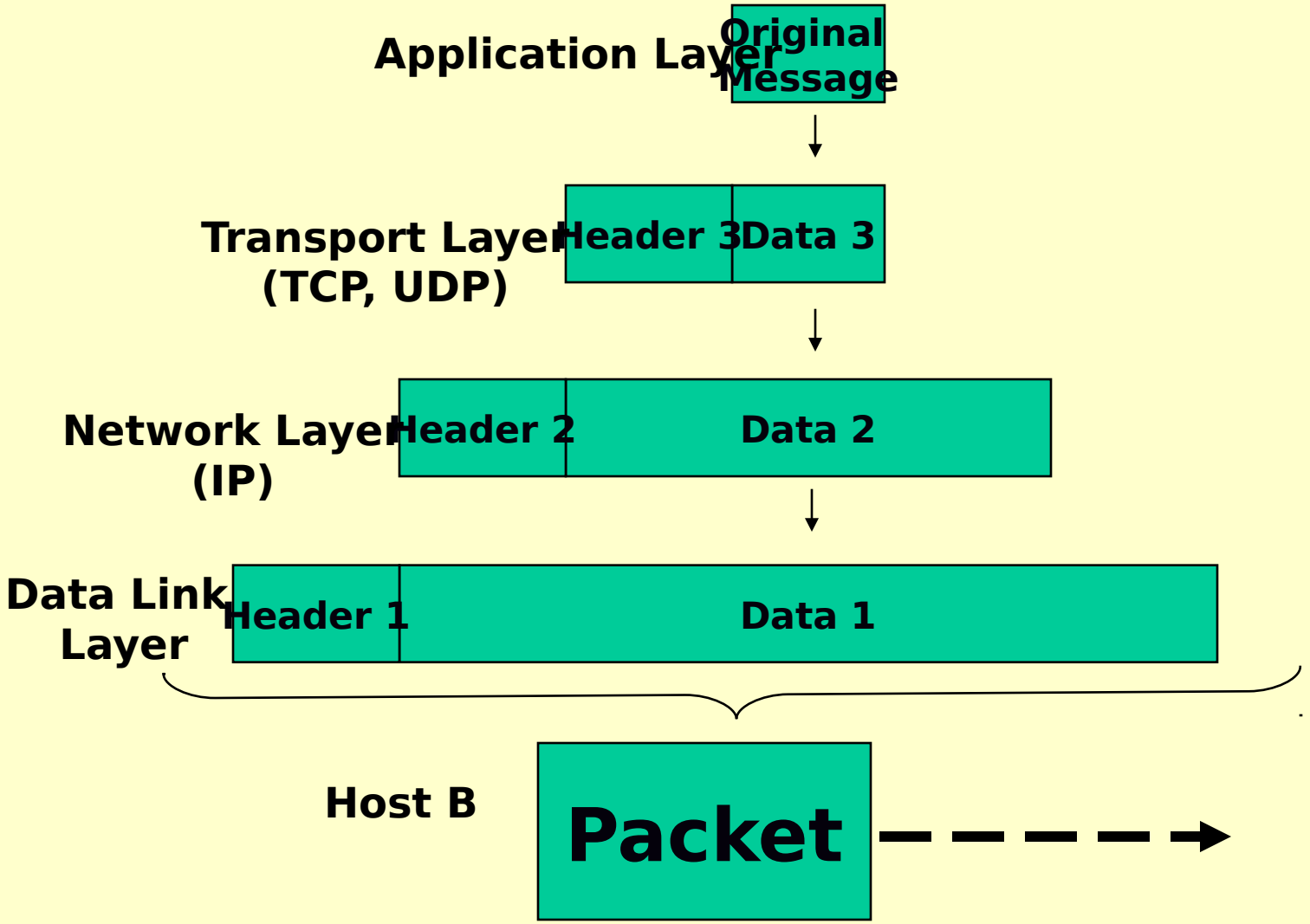
TCP/IP


Application Layer
Original Message
Transport Layer (TCP, UDP)
Header 3
Data 3
Network Layer (IP)
Header 2
Data 2
Data Link Layer
Header 1
Data 1
Host A
Packet

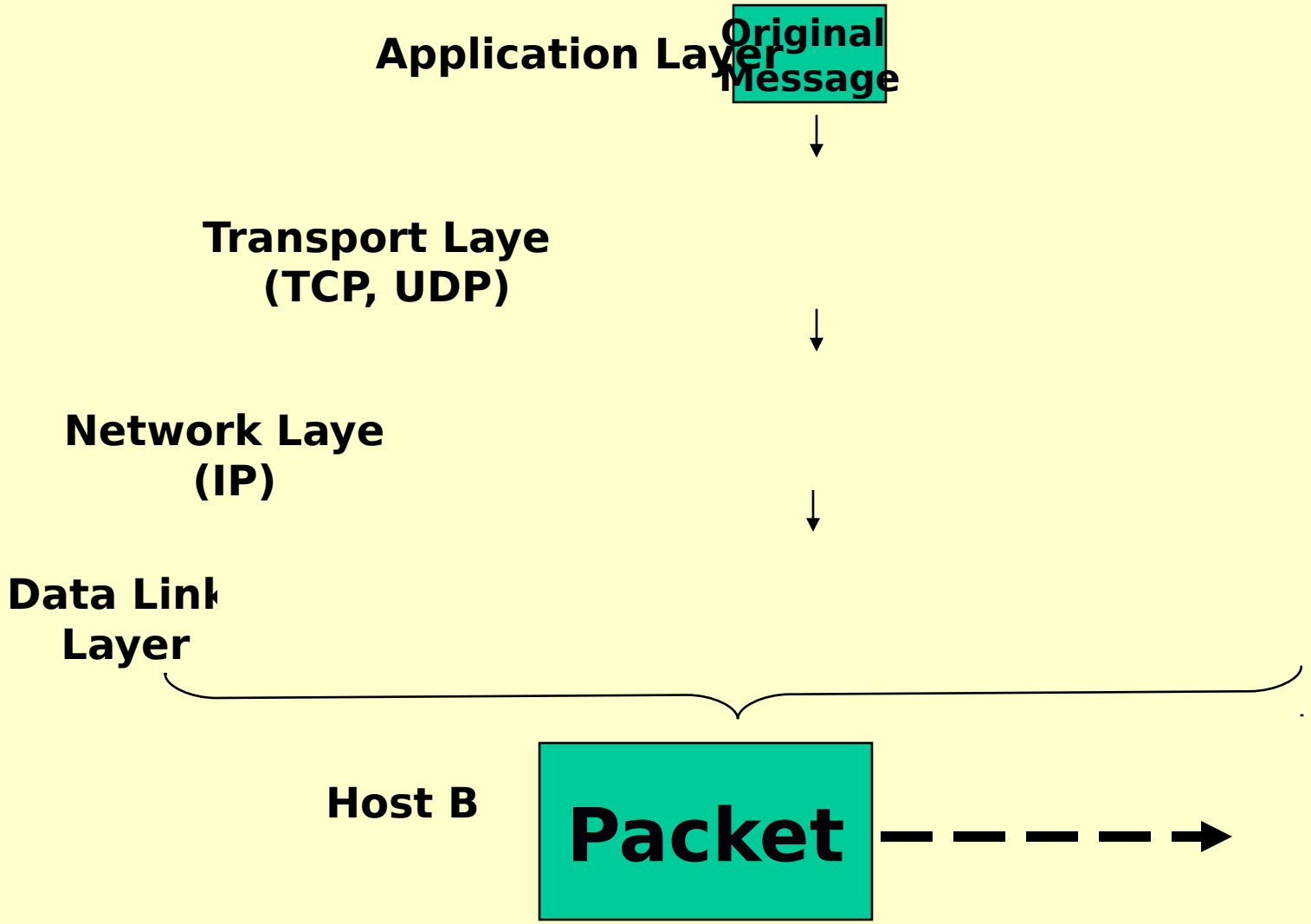
TCP/IP


Network Layer
Data Link Layer
Packet
Data Link Layer
Header 1
Data 1
Host B

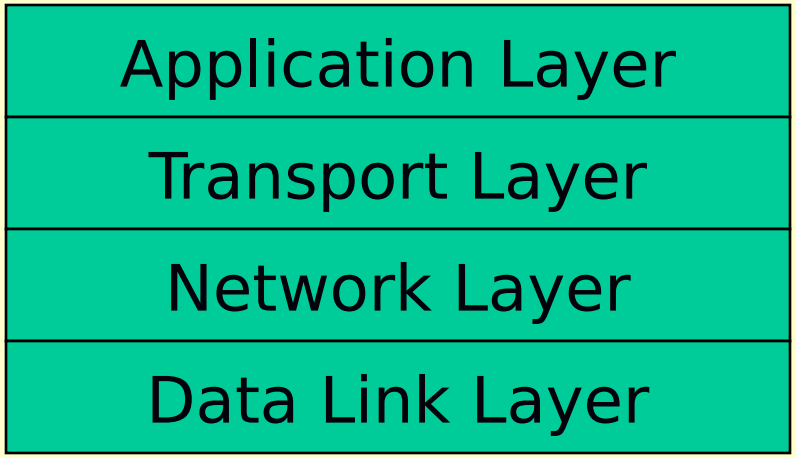
TCP/IP


Application Layer
Original Message
Transport Layer (TCP, UDP)
Header 3
Data 3
Network Layer (IP)
Header 2
Data 2
Data Link Layer
Header 1
Data 1
Host B
Packet

TCP/IP


Application Layer
Original Message
Transport Laye (TCP, UDP)
Network Laye (IP)
Data Link Layer
Host B
Packet

Security at What Level?



PGP, Kerberos, SSH, etc.

Transport Layer Security (TLS)

IP Security

Hardware encryption

Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Virtual Private Network (VPN)

- A group of two or more computer systems, typically connected to a private network with limited public-network access that communicates “securely” over a public network
- A combination of tunneling, encryption, authentication and access control technologies and services used to carry traffic over an IP network

VPN Advantages

- Ubiquitous Coverage
- Cost Reduction
- Security
- E-Commerce

VPN Types and Architecture

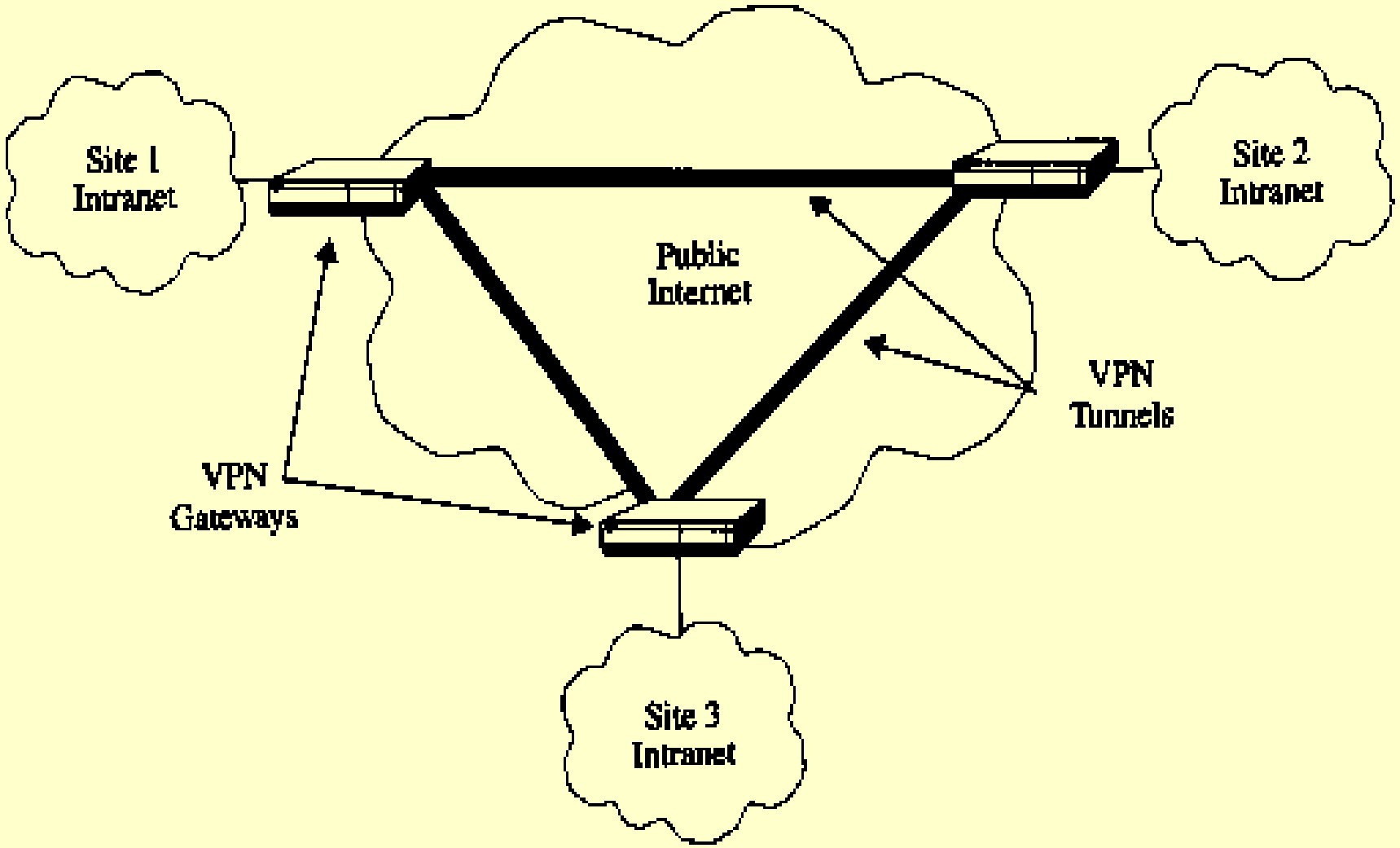
Types:

- Hardware based
- Firewall based
- Standalone/Software based

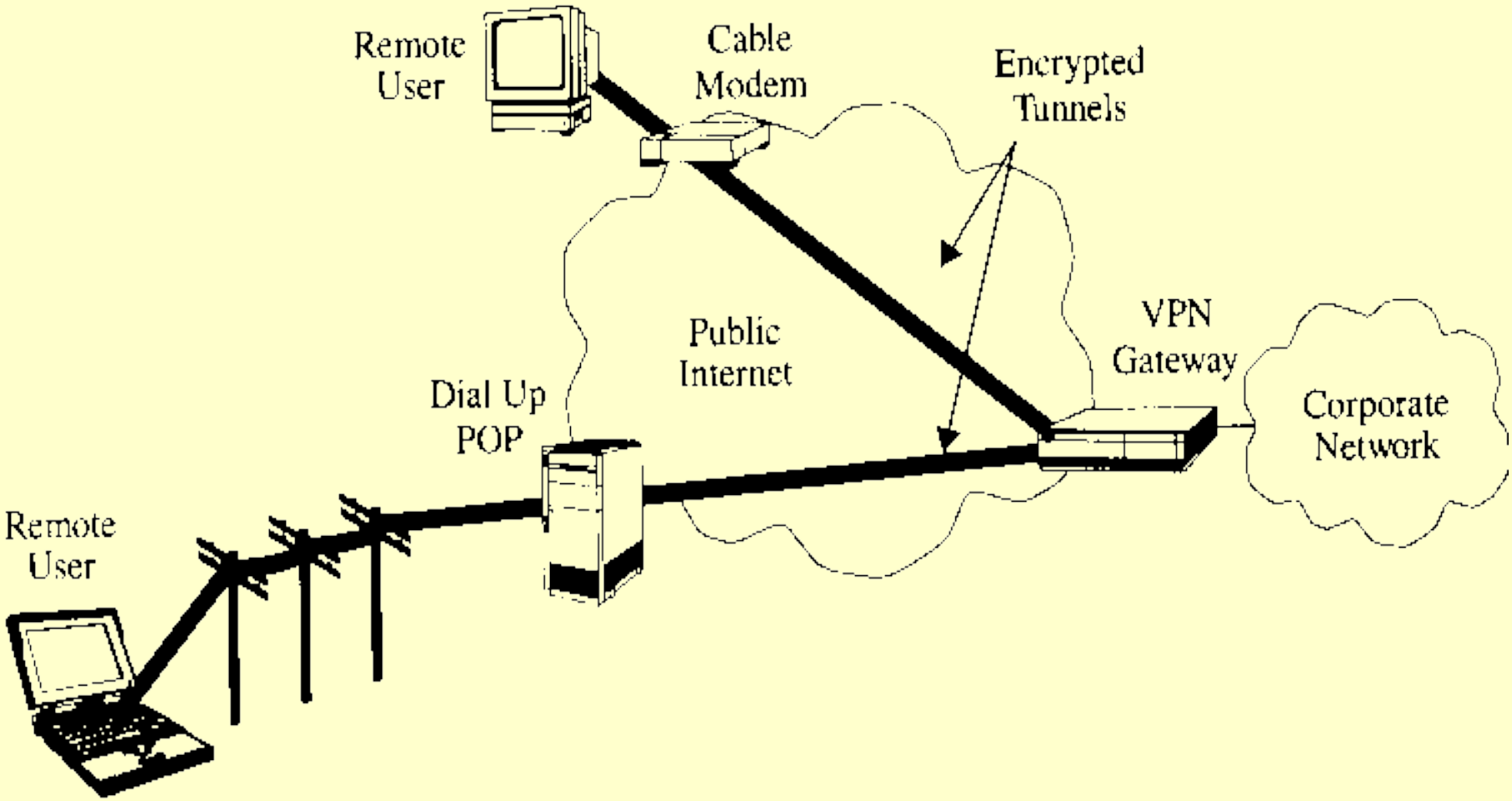
Architecture: (next 3 slides)

- Site-to-Site
- Remote Access
- Extranet

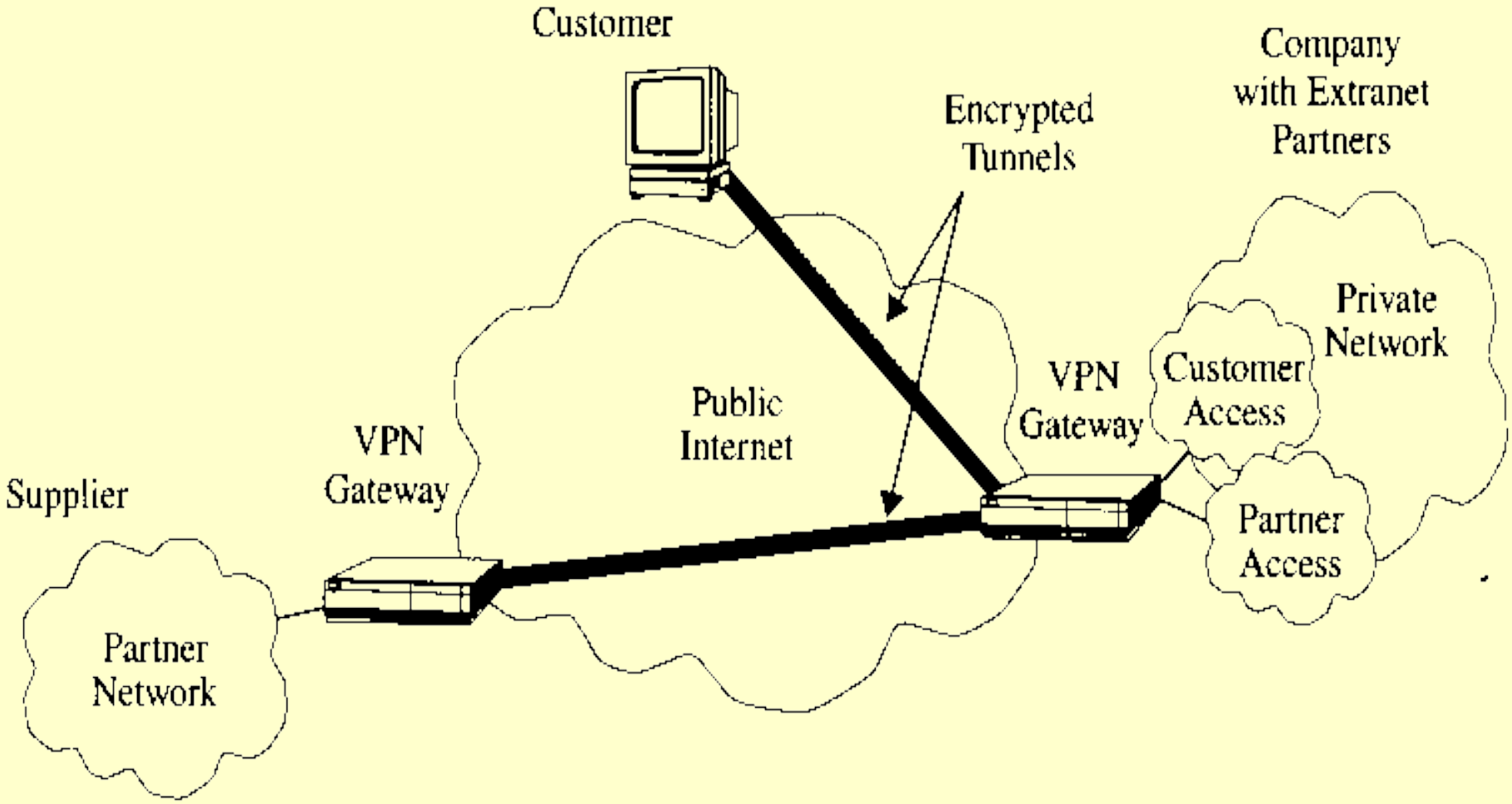
Site-to-Site Intranet VPN



Remote Access VPN



Extranet VPN



Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Security at Data Link Layer

- (Hardware encryption)
- Need a dedicated link between host/routers.

- Advantages

- Speed.

- Disadvantages

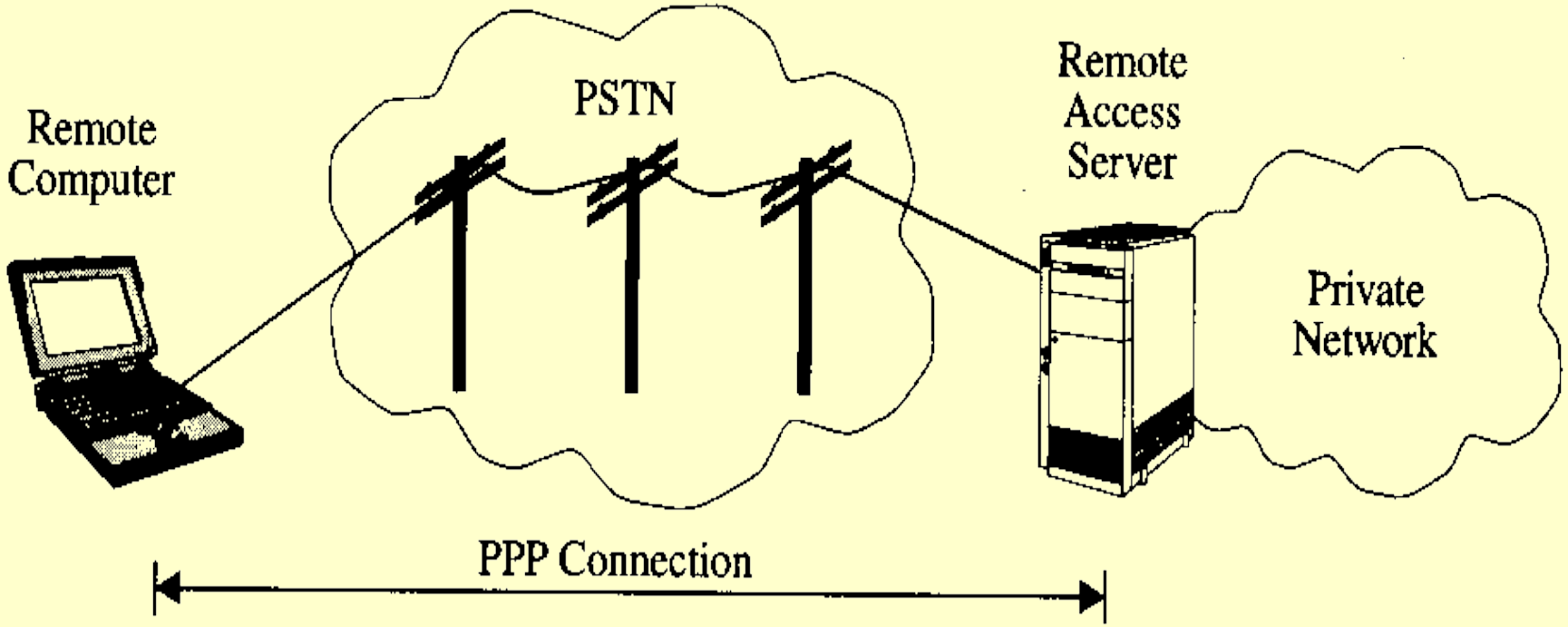
- Not scalable.
- Need dedicated links.

Layer 2 VPN

- Tunneling
- Point-to-Point Tunnel Protocol (PPTP)
- Layer 2 Forwarding Protocol (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Layer 2 Authentication

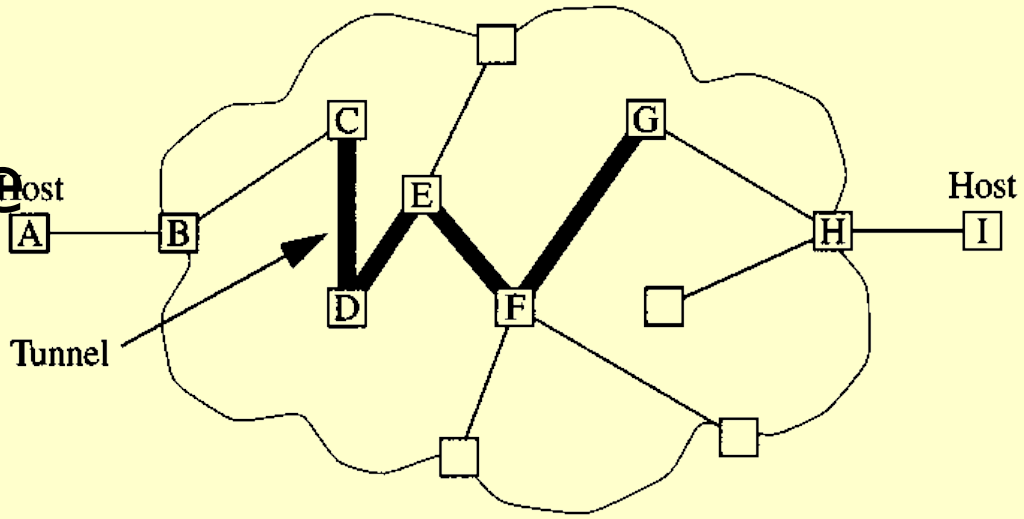
Tunneling (1 of 2)

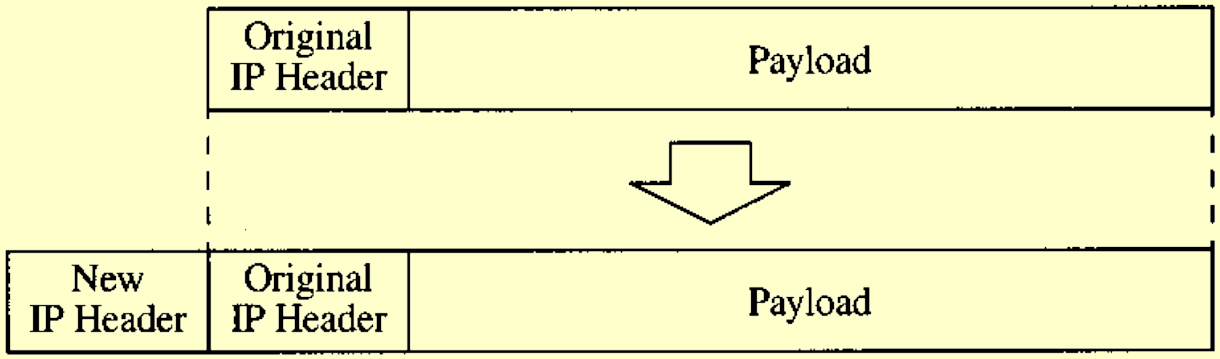
- Developed primarily for remote users
- Reduces long distance phone charges
- Reduces hardware costs (i.e. modem banks)
- Security (confidentiality and authentication) is marginal



Tunneling (2 of 2)

Encapsulation of a data packet (original) so the inner packet is opaque to the network over which the outer packet is routed

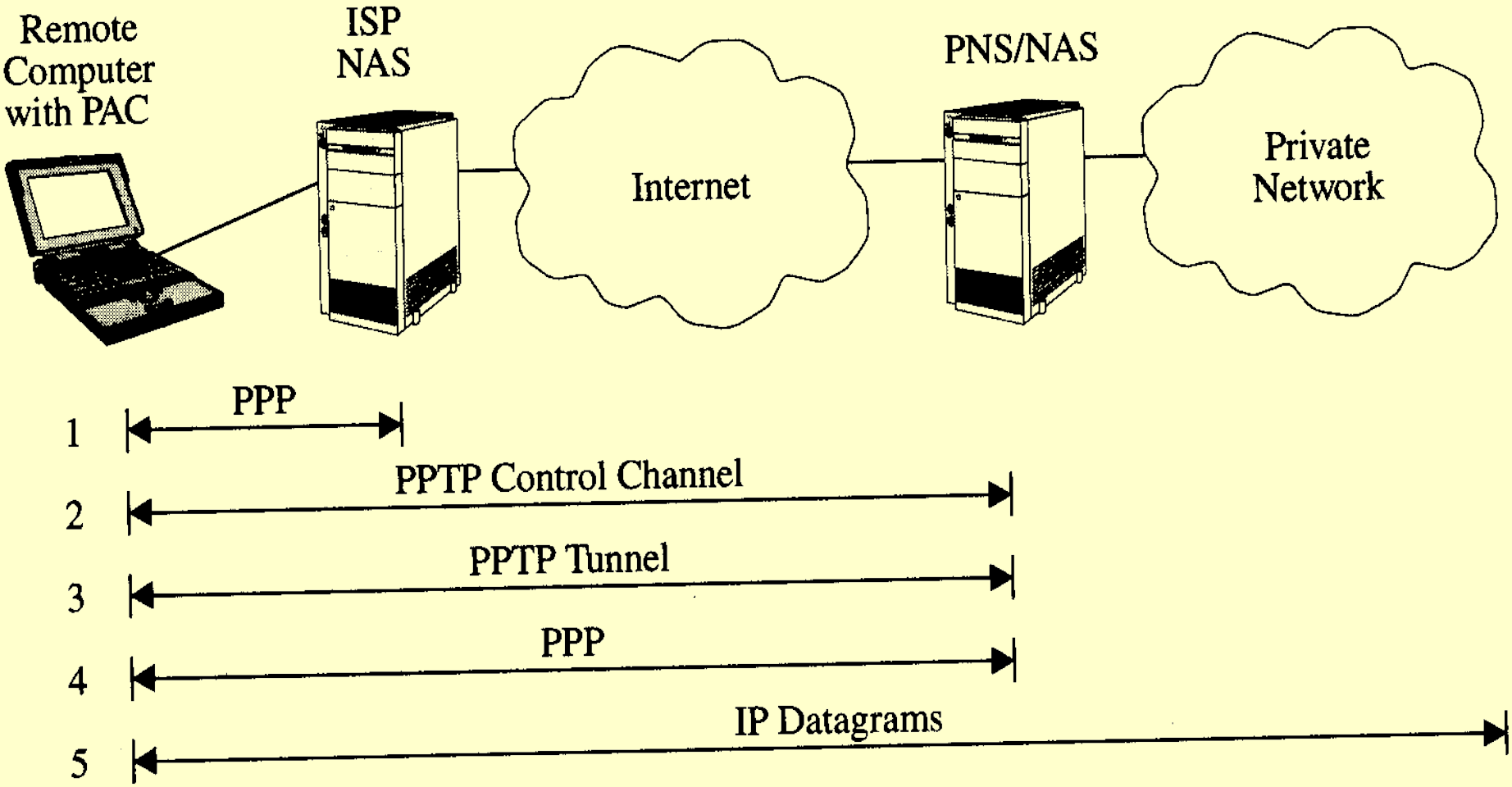




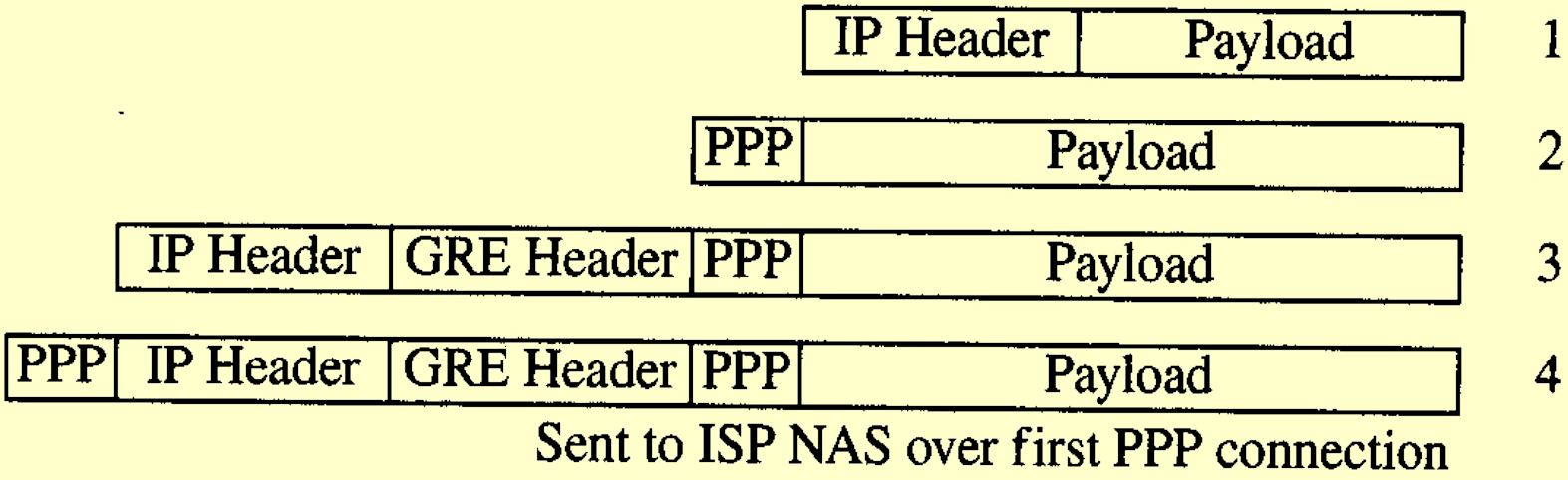
Point-to-Point Tunneling Protocol (PPTP) (1 of 3)

- Developed by consortium that included Microsoft, 3COM, US Robotics, Ascend Communications (1996)
- Requires Point-to-Point Protocol (PPP) and IP packets
- Uses Microsoft Point-to-Point Encryption (MPPE) for confidentiality/encryption, but MPPE is flawed
- Uses CHAP, PAP or EAP for authentication
- No message authentication
- Utilizes Generic Routing Encapsulation – can support other layer 3 protocols (IPX, AppleTalk)
- Allows only one simultaneous connection

PPTP (2 of 3)


Remote Computer with PAC
ISP NAS
Internet
PNS/NAS
Private Network
1
PPP
2
PPTP Control Channel
3
PPTP Tunnel
4
PPP
5
IP Datagrams

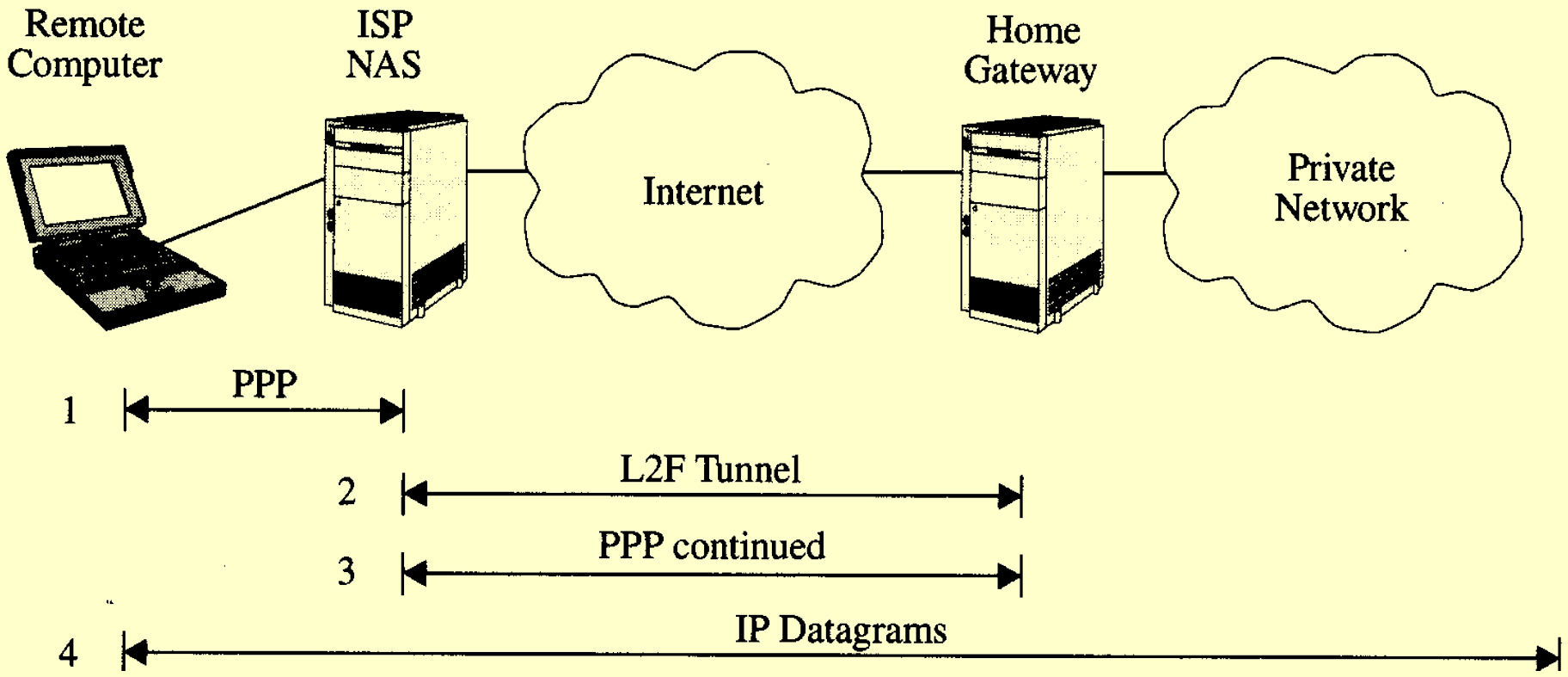
PPTP (3 of 3)


IP Header
Payload
1
PPP
Payload
2
IP Header
GRE Header
PPP
Payload
3
PPP
IP Header
GRE Header
PPP
Payload
4
Sent to ISP NAS over first PPP connection
IP Header
GRE Header
PPP
Payload
5
Sent across Internet to PNS (PPTP Tunnel)
PPP
Payload
6
PNS terminates second PPP connection
IP Header
Payload
7
Sent to destination host over intranet

Layer 2 Forwarding Protocol (L2F)

- Similar to PPTP
- Requires PPP but can use frame relay, ATM or X.25 instead of IP
- Supports additional authentication standards
  - Terminal Access Control Access Control System (TACACS+)
  - Remote Authentication Dial-In User Service (RADIUS)
- Allows multiple simultaneous connections

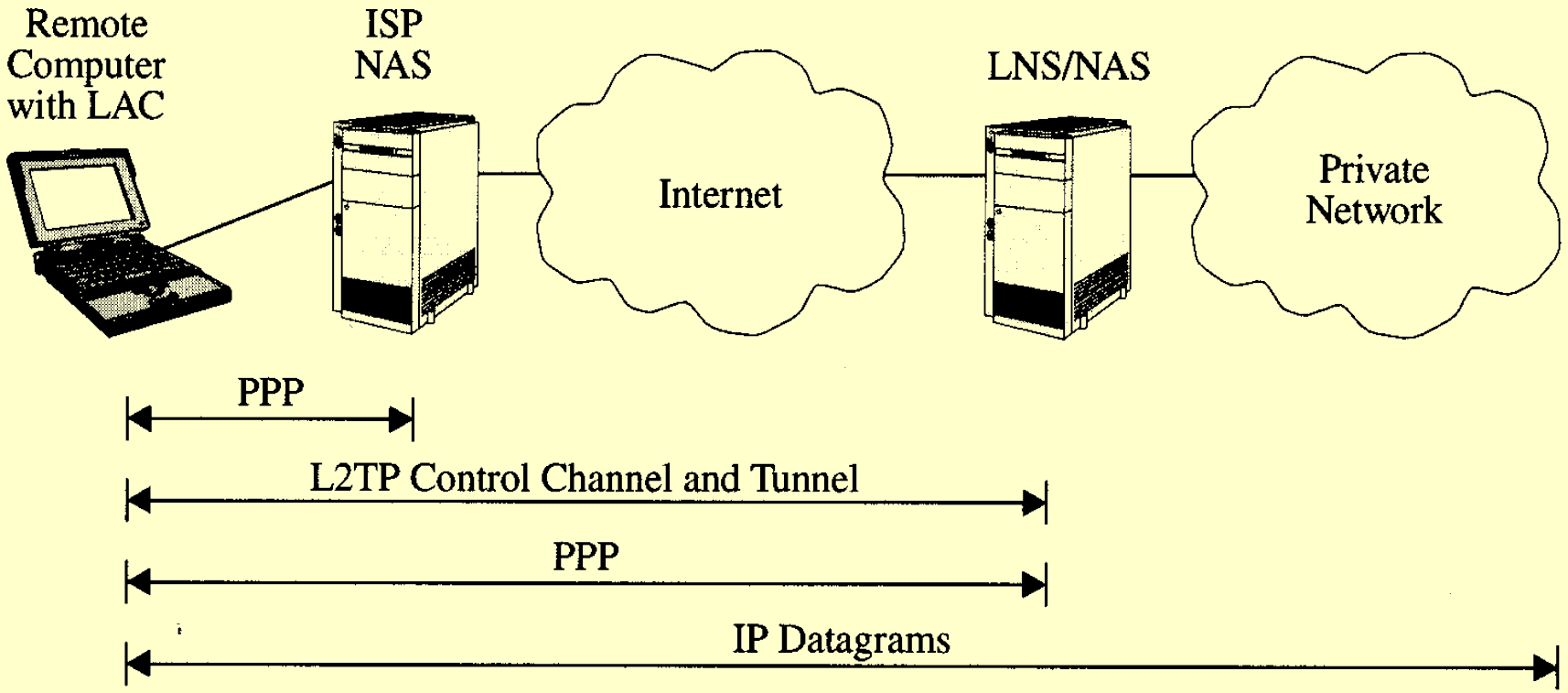
Layer 2 Forwarding Protocol (L2F)



Layer 2 Tunneling Protocol (L2TP)

- Combines best of L2F and PPTP
- Requires PPP but can use either IP, frame relay, X.25 or ATM
- Almost always used with IPSec since L2TP provides no confidentiality or message authentication
- With IP, it uses UDP port 1701
- Allows multiple simultaneous connections
- Only layer 2 tunneling protocol that is IPSec compliant

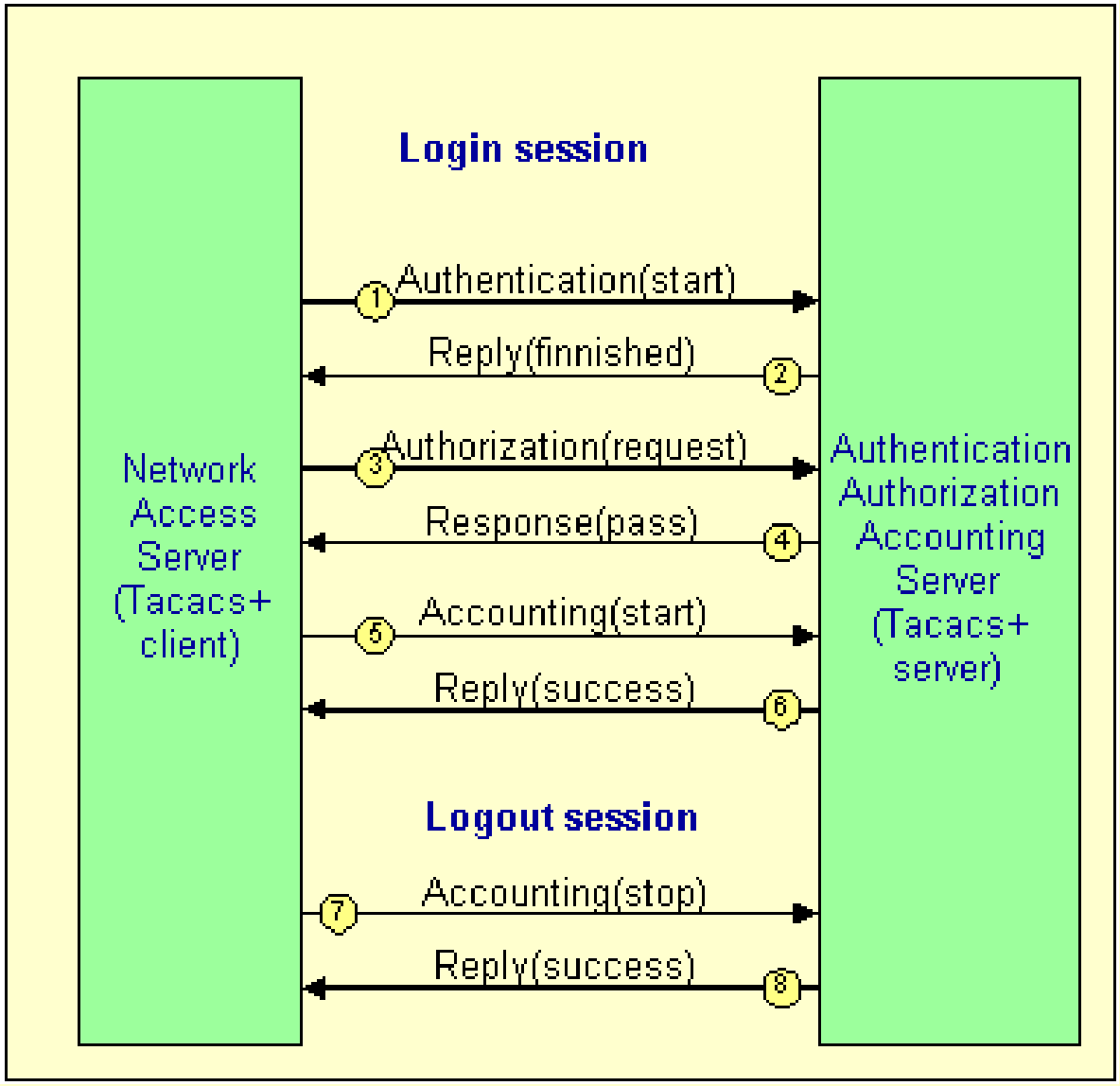
Layer 2 Tunneling Protocol (L2TP)



Layer 2 VPN Authentication Protocols

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Extensible Authentication Protocol (EAP)
- Remote Access Dial In User Service (RADIUS)
- Terminal Access Controller Access Control System (TACAS/TACACS+)

TACACS+ Message Flow



Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols
- (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Security at Network Layer

IP Security (IPSec)

- Advantages

- Provides seamless security to application and transport layers (ULPs).
- Allows per flow or per connection security and thus allows for very fine-grained security control.

- Disadvantages

- More difficult to to exercise on a per user basis on a multi-user machine.

Why IPSEC?

- IP Packets have no inherit security
- Can easily
  - Forge IP addresses
  - Modify packets
  - Replay packets
  - Inspect packets in transit
- No guarantee that IP packets:
  - Are from the claimed sender
  - Contain data that sender placed into them
  - Not inspected by a third party while in transit

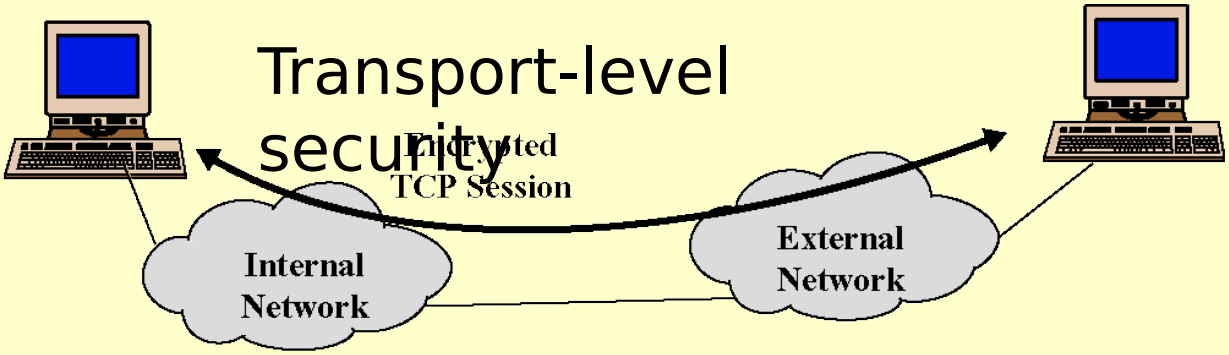
IP Security (IPSEC)

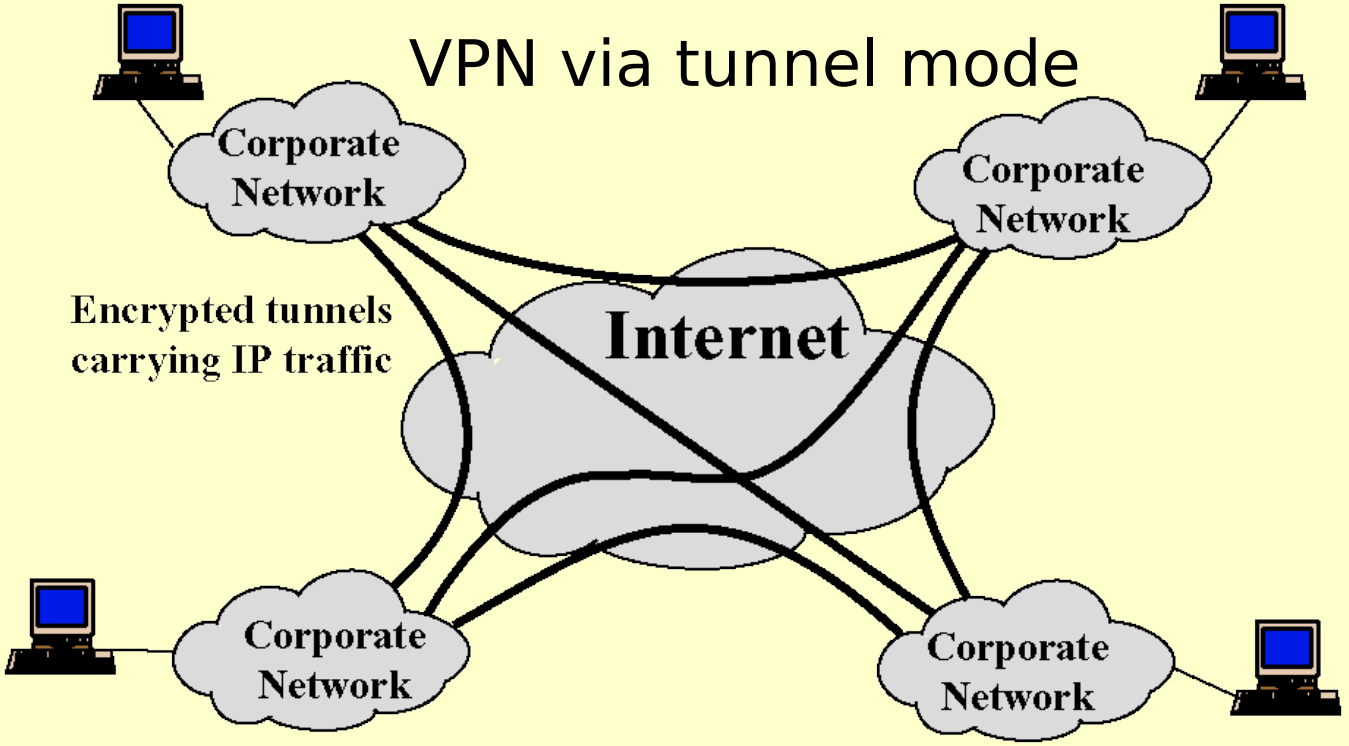
- Communication Modes
- Comprised of:
  - IP Header
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Can operate in three modes
  - AH only
  - ESP only
  - AH and ESP combined (for tunneling mode)
- IPSEC Keying

Communication Modes

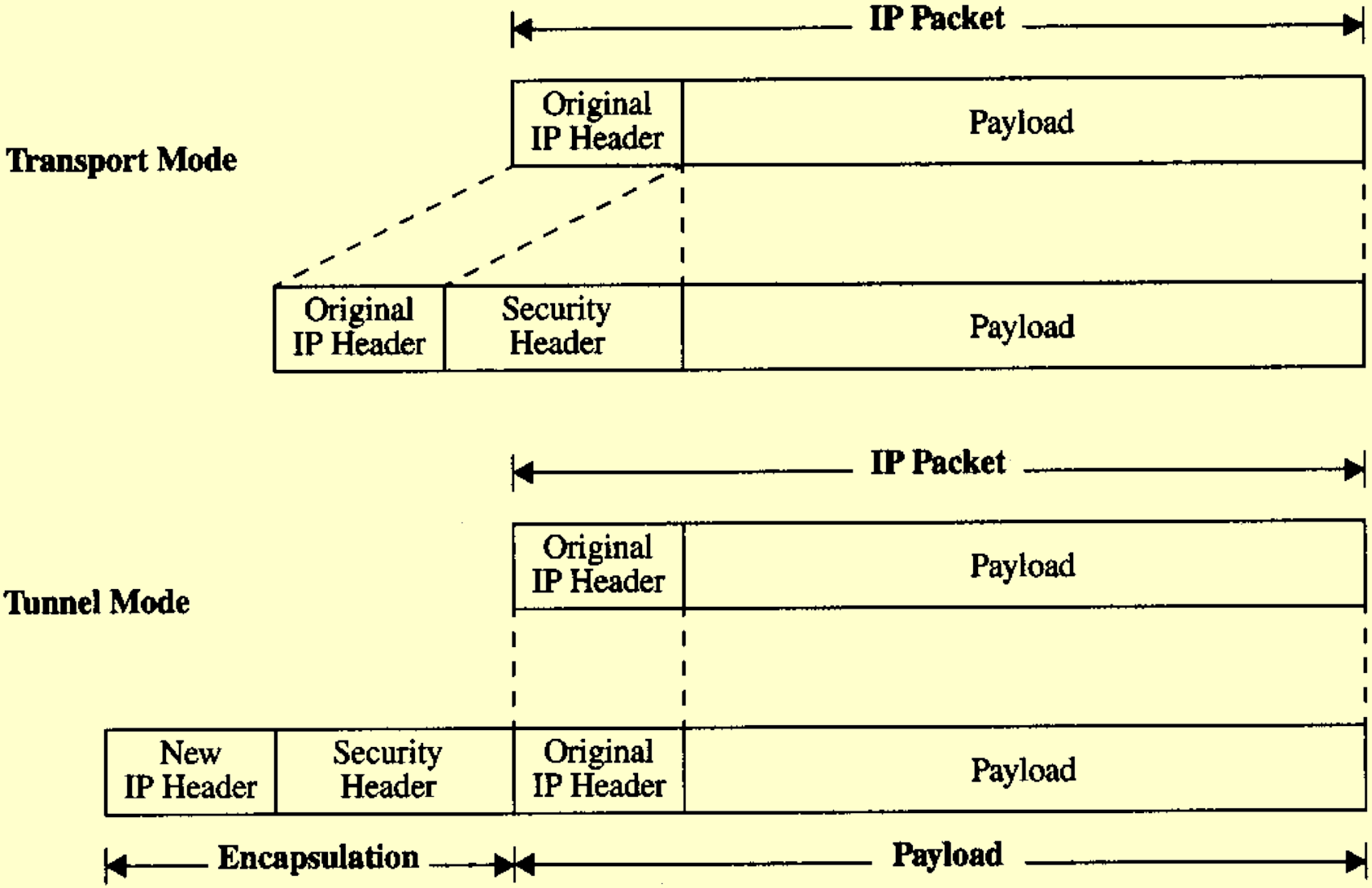
- Transport
  - Original IP header is not changed
  - Endpoints normally terminate at workstations
  - Possible to perform traffic analysis
- Tunnel
  - Entire original IP packet is encapsulated
  - Encryption is only partial path
  - Endpoints normally terminate at routers or firewalls
  - Significantly increases size of IP packet

Transport and Tunnel Mode





Transport and Tunnel Modes

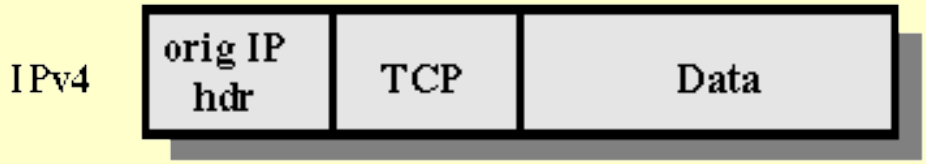


IPSEC Protocols

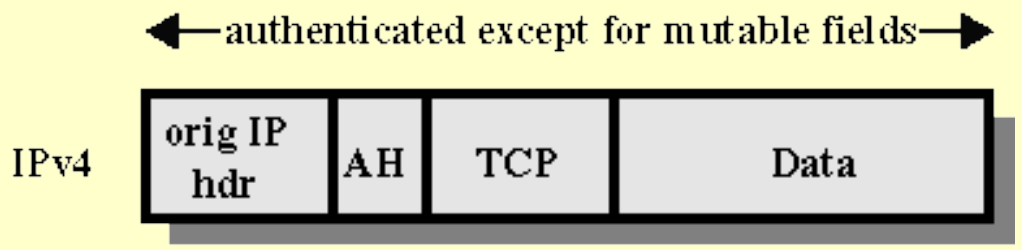
Authentication Header

- Provides authentication and integrity
- Does not provide confidentiality
- Uses HMAC algorithms
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- Packet must be reassembled before authentication

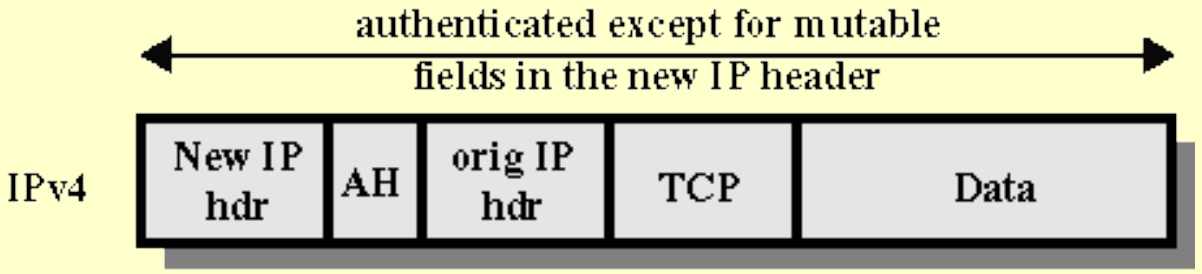
AH Authentication



Before applying AH



Transport Mode

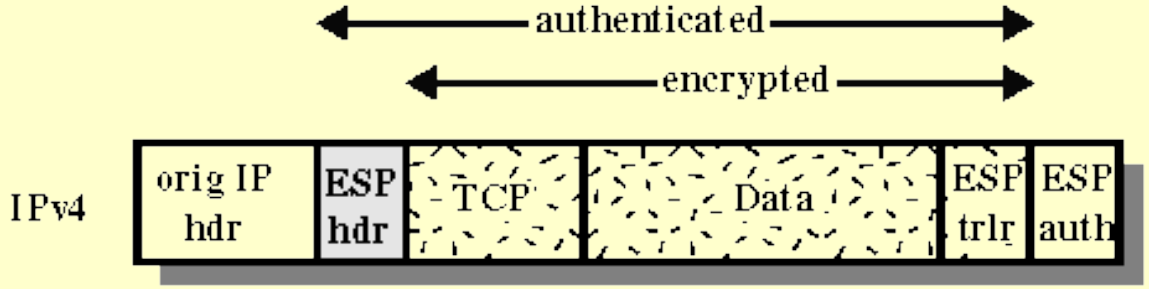


Tunnel Mode

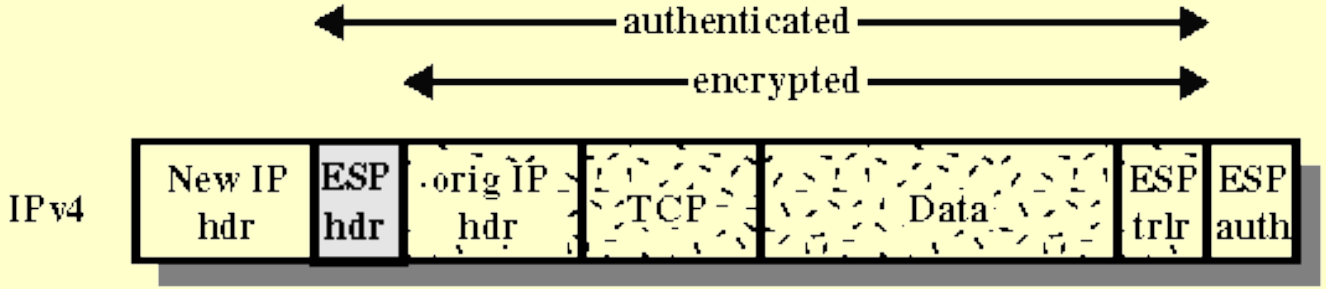
Encapsulating Security Payload (ESP)

- Provides confidentiality
- Can support the following cryptographic algorithms
  - DES
  - 3DES
  - IDEA
  - 3IDEA
  - CAST
  - Blowfish
- Default is DES-CBC
- Can also support authentication with HMAC

ESP Encryption and Authentication

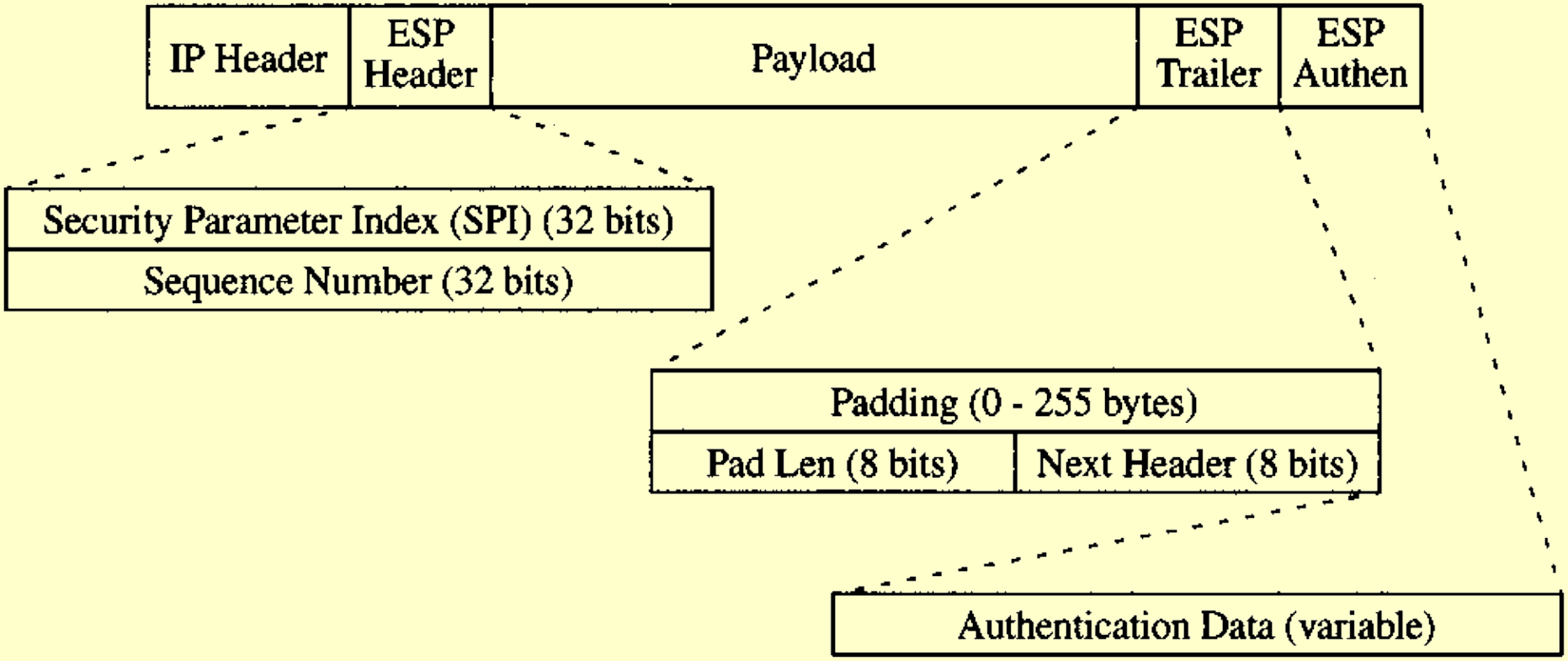


Transport Mode



Tunnel Mode

ESP Format


IP Header
ESP Header
Payload
ESP Trailer
ESP Authen
Security Parameter Index (SPI) (32 bits)
Sequence Number (32 bits)
Padding (0 - 255 bytes)
Pad Len (8 bits)
Next Header (8 bits)
Authentication Data (variable)

IPSec Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

IPSec Keying

- Manual
  - Pre-placed
  - Shared password
  - X.509 certificate
- Automatic
  - Internet Key Exchange (IKE)

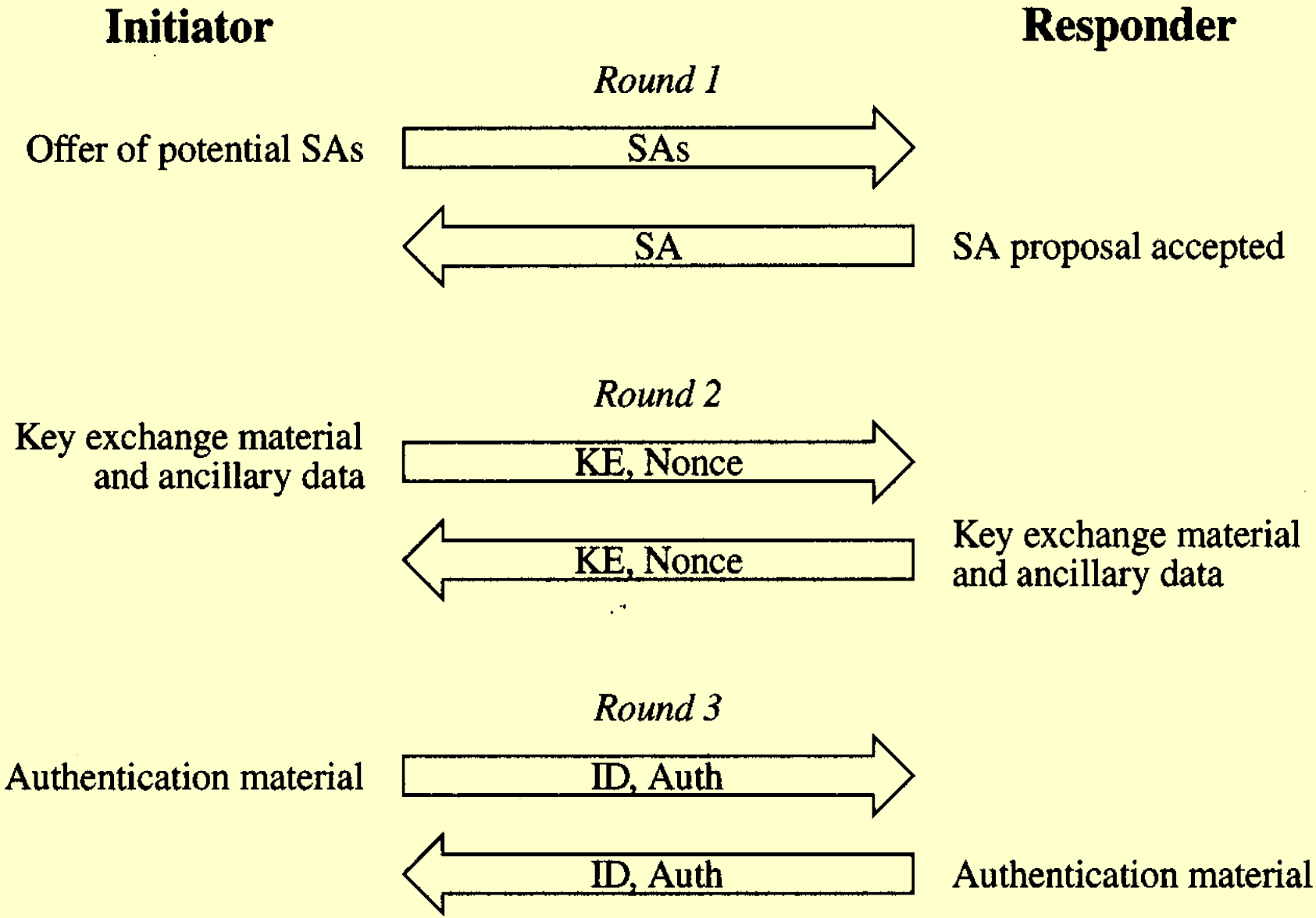
Internet Key Exchange (IKE)

- Dynamic generation of keys for IPSec protocols
- Composed of three protocols
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Secure Key Exchange Mechanism (SKEME)
  - Oakley Key Determination Protocol
- RFC2409

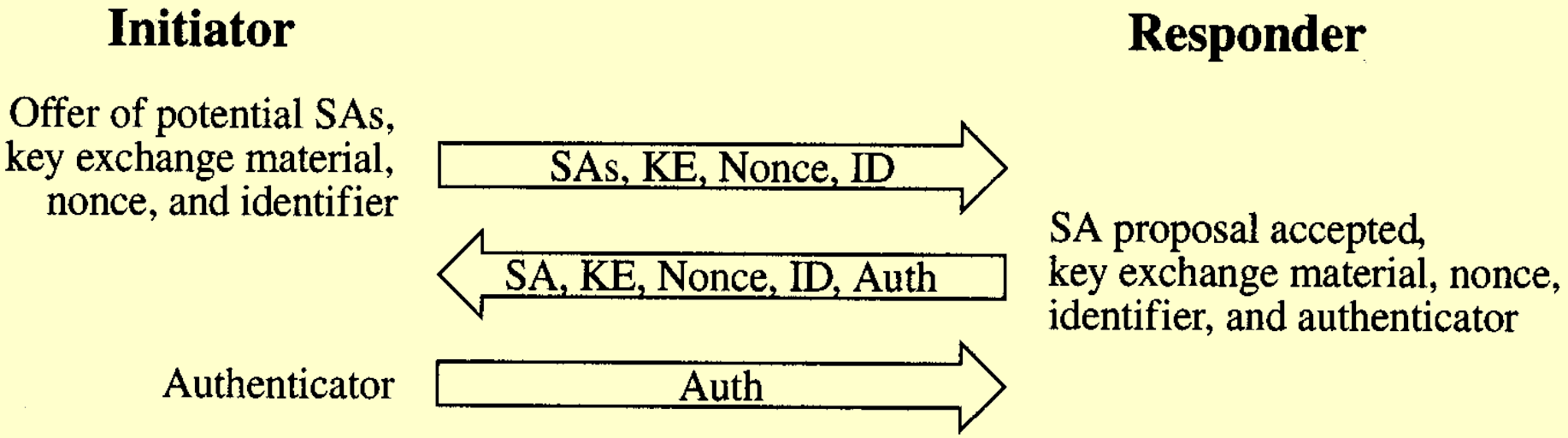
IPSec Security Process

- Phase I – Creation of IKE SA
- Phase 2 – Creation of IPSec SAs

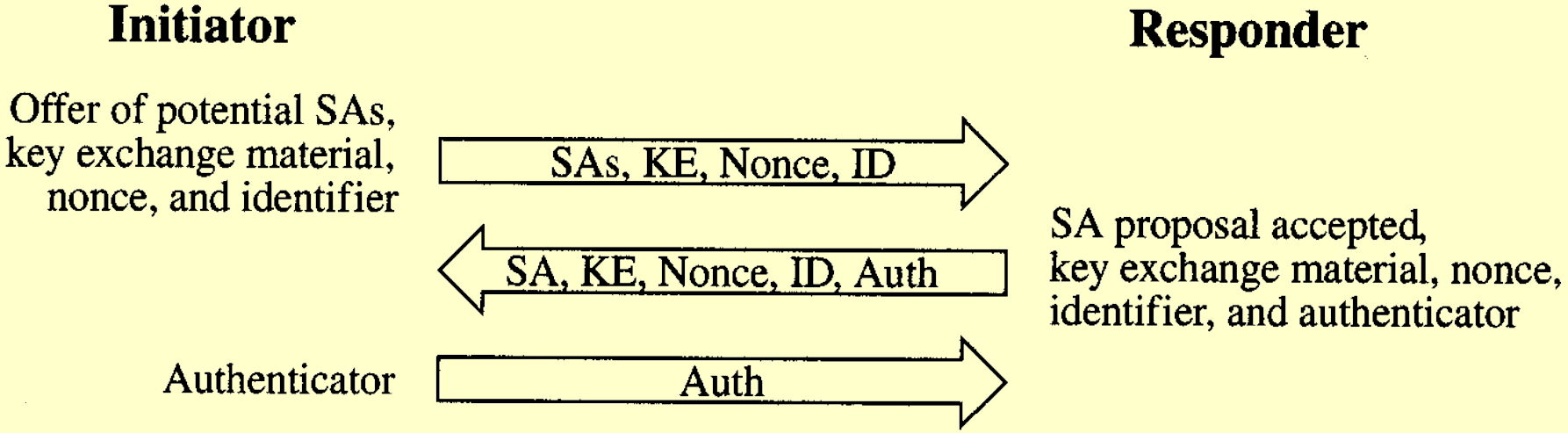
IKE Phase 1/Main Mode



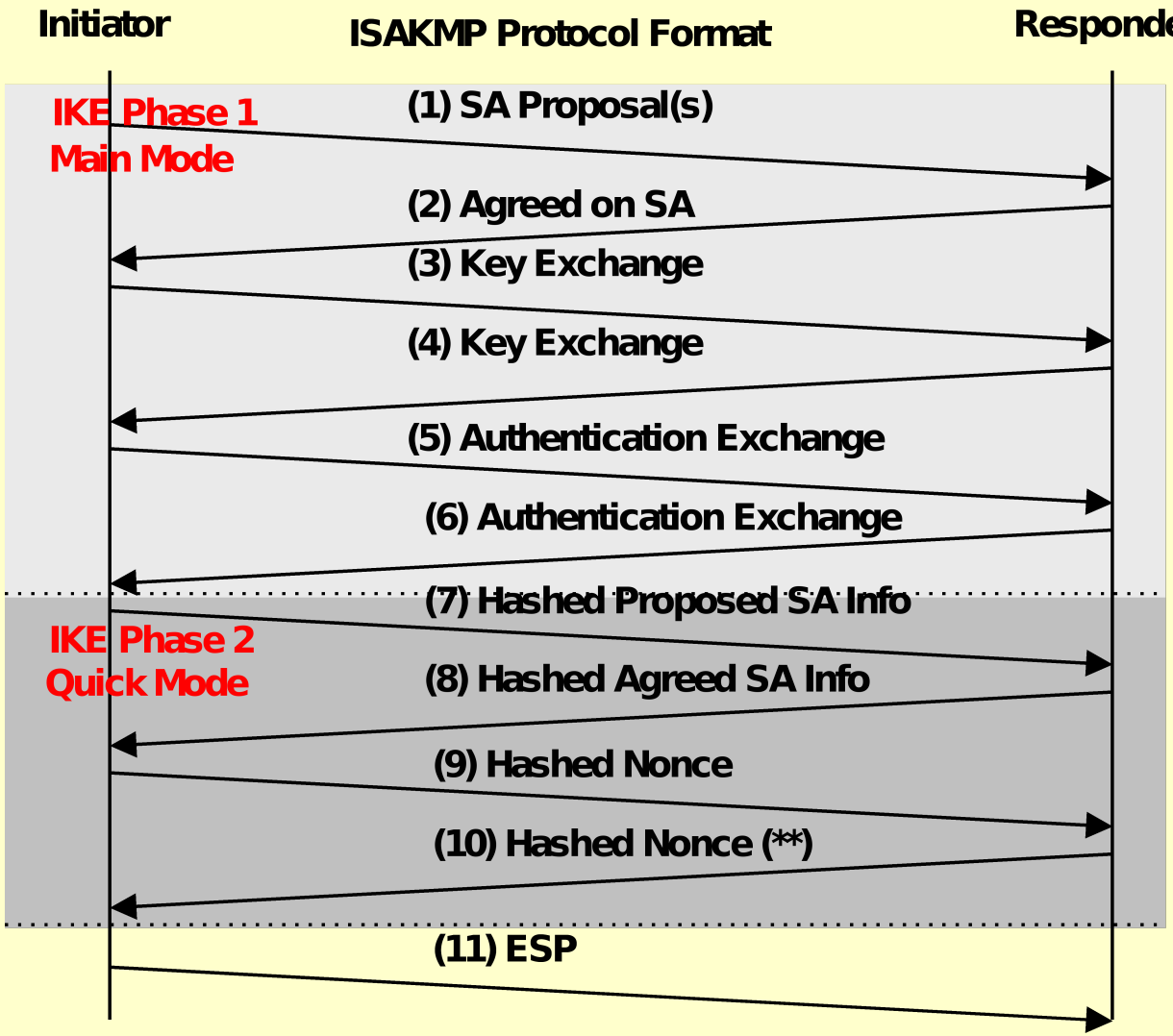
IKE Phase I Aggressive


Initiator
Responder
Offer of potential SAs, key exchange material, nonce, and identifier
SAs, KE, Nonce, ID
SA, KE, Nonce, ID, Auth
SA proposal accepted, key exchange material, nonce, identifier, and authenticator
Authenticator
Auth

IKE Phase 2/Quick Mode (IPSec)


Initiator
Responder
Offer of potential SAs, key exchange material, nonce, and identifier
SAs, KE, Nonce, ID
SA, KE, Nonce, ID, Auth
SA proposal accepted, key exchange material, nonce, identifier, and authenticator
Authenticator
Auth

Internet Key Exchange



**A three way handshake may be used eliminating the need for packet 10.

Oakley Key Determination Protocol

- Specific key exchange algorithm mandated for use with initial version of ISAKMP
- Refinement of Diffie-Hellman key exchange algorithm
  - Authentication
  - Cookies (hash of source and destination IP address and ports)
  - Nonce (pseudorandom number to prevent replay attacks)

Internet Security Association and Key Management Protocol (ISAKMP)

- Provides means to:
  - Authenticate a peer
  - Exchange information for key exchange
  - Negotiate security services
- Does not define the following
  - How a particular authenticated key exchange is done
  - Define attributes necessary for SA establishment
- Establishes but is independent of the key exchange protocol, encryption algorithm or authentication method
- Uses UDP port 500

IPSec Advantages and Disadvantages

- Standard method allows vendor interoperability, but may cause incompatibilities
- Open protocols allows flexibility
- Supports encryption, authentication and key management.
- Problems with NAT and AH (NAT changes source IP which cause the MAC to be invalid at distant end)
- Routing and addressing challenges
- However, best current solution for lower level encryption

Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Security at Transport Layer

Transport Layer Security (TLS)

- Implemented in end-hosts
- Advantages
  - Existing applications get security seamlessly
- Disadvantages
  - Protocol specific

Security at Application Layer

(PGP, Kerberos, SSH, etc.)

- Implemented in end-hosts
- Advantages

- Extend application without involving operating system.
- Application can understand the data and can provide the appropriate security.

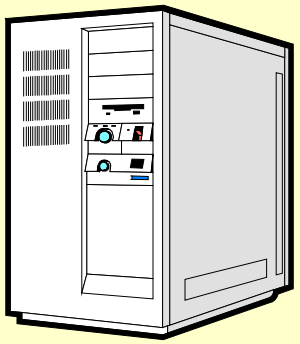
- Disadvantages

- Security mechanisms have to be designed independently of each application.

Secure Shell (SSH)

- Performs client authentication
- Safeguards multiple service sessions between two systems
- Uses port 22
- Validates users credentials
- Uses 3DES

SSH Process



Client requests SSH link

Each side sends protocol version

Key exchange & algorithm negotiation

Encrypted Link

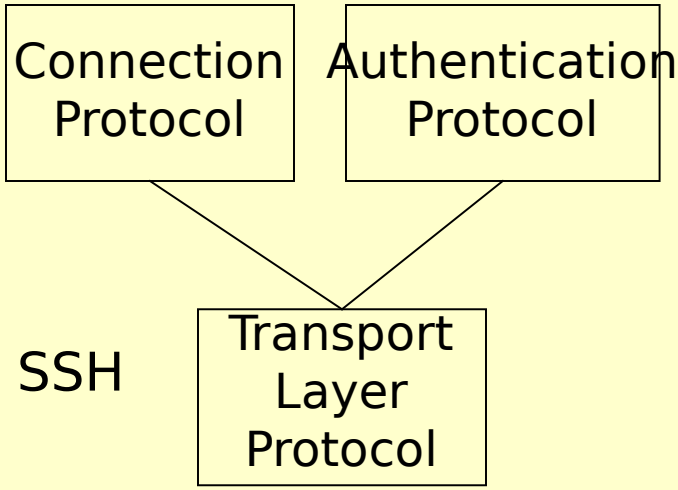
Client requests service

SSH Versions

- Two versions of SSH
  - SSH-1
    - Flaws
    - Monolithic
  - SSH-2
    - More secure
    - Modular

SSH-2 Architecture

- Transport Layer Protocol
  - Encryption
  - Authentication
  - Integrity
  - Compression
- Connection Protocol
  - Allows clients to negotiate additional channels through SSH tunnel
  - Multiplex
  - Decreases overhead
- Authentication Protocol
  - Authenticates user
  - Not always needed



Secure Socket Layer (SSL) and Transport Layer Security (TLS)

- SSL and TLS are Session, Presentation, and Application layer protocols that provide web security
  - HTTP
  - FTP
  - SMTP
  - Any other TCP based application
- SSLv3 is the older standard developed by Netscape
- SSL/TLS provides confidentiality and integrity
- TLS is the new IETF standard

SSL Protocol

- The primary goal is to provide privacy and reliability between two communicating applications.
- The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Secure Socket Layer (SSL)

- Created by Netscape
- Encrypts at the OSI Layer 5 (session layer)
- Used for e-commerce
- Encrypts with RSA
- Web page developers can flag page requiring SSL

SSL

- Designed with four basic goals
  - Cryptographic security
  - Interoperability
  - Extensibility
  - Relative efficiency

SSL

SSL has three basic properties:

- The connection is private.
- The peer's identity can be authenticated.
- The connection is reliable.

SSL/TLS

- What is TLS?
  - Transport Layer Security (version 1.0)
- SSL was developed by Netscape.
- Thus was born TLS
  - IETF changed the name to avoid showing bias

SSL/TLS

- The TLS protocol provides communications privacy over the Internet.
- The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
- Sound familiar?
- TLS v1.0 == SSL v3.1

SSL/TLS

- Users want to connect to servers without the connection being listened to
  - Units/Organizations
  - Electronic commerce
  - University (Grades)
- Every server has a certificate
  - Basically a public key
  - Signed by a trusted third party

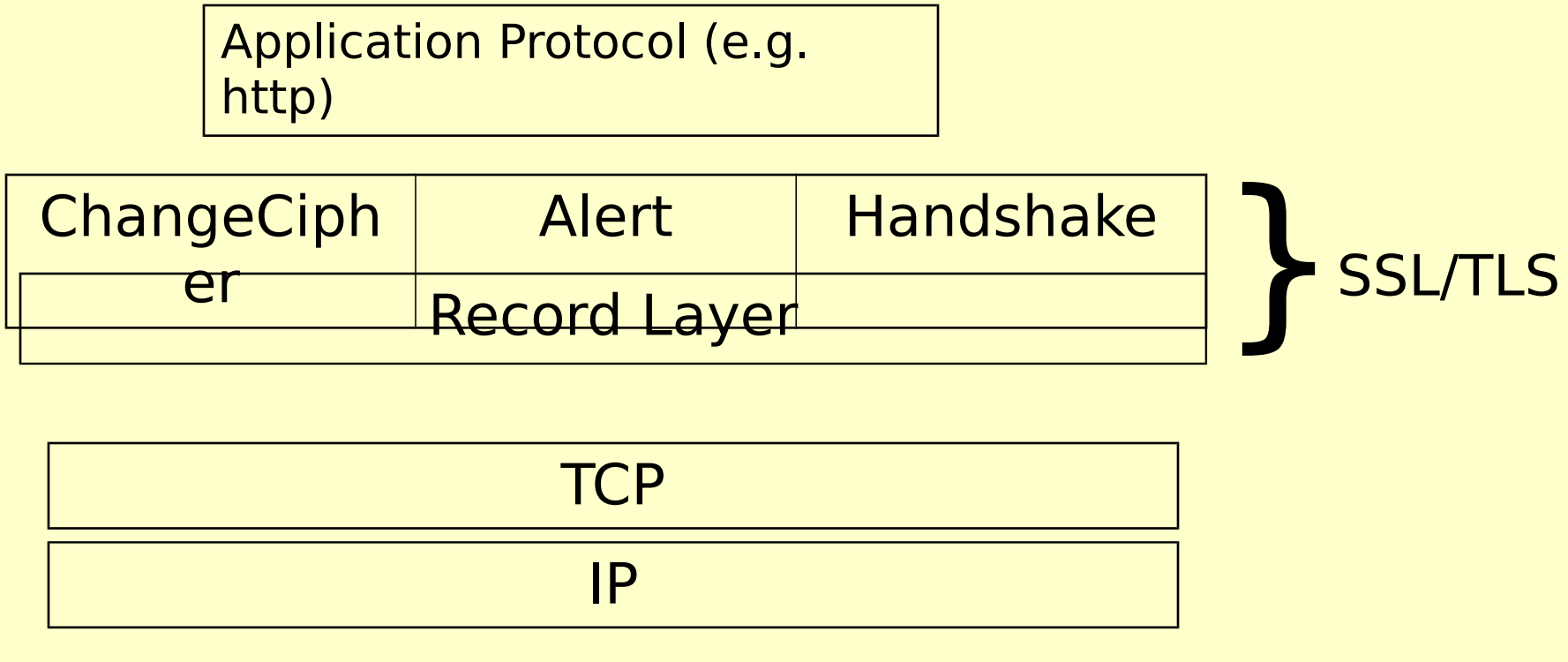
Server Certificates

- X.509 version 3 is the current specification
- Certificates hold three important bits of information
  - Name of Server
  - Public Key of Server
  - Issued by a trusted organization

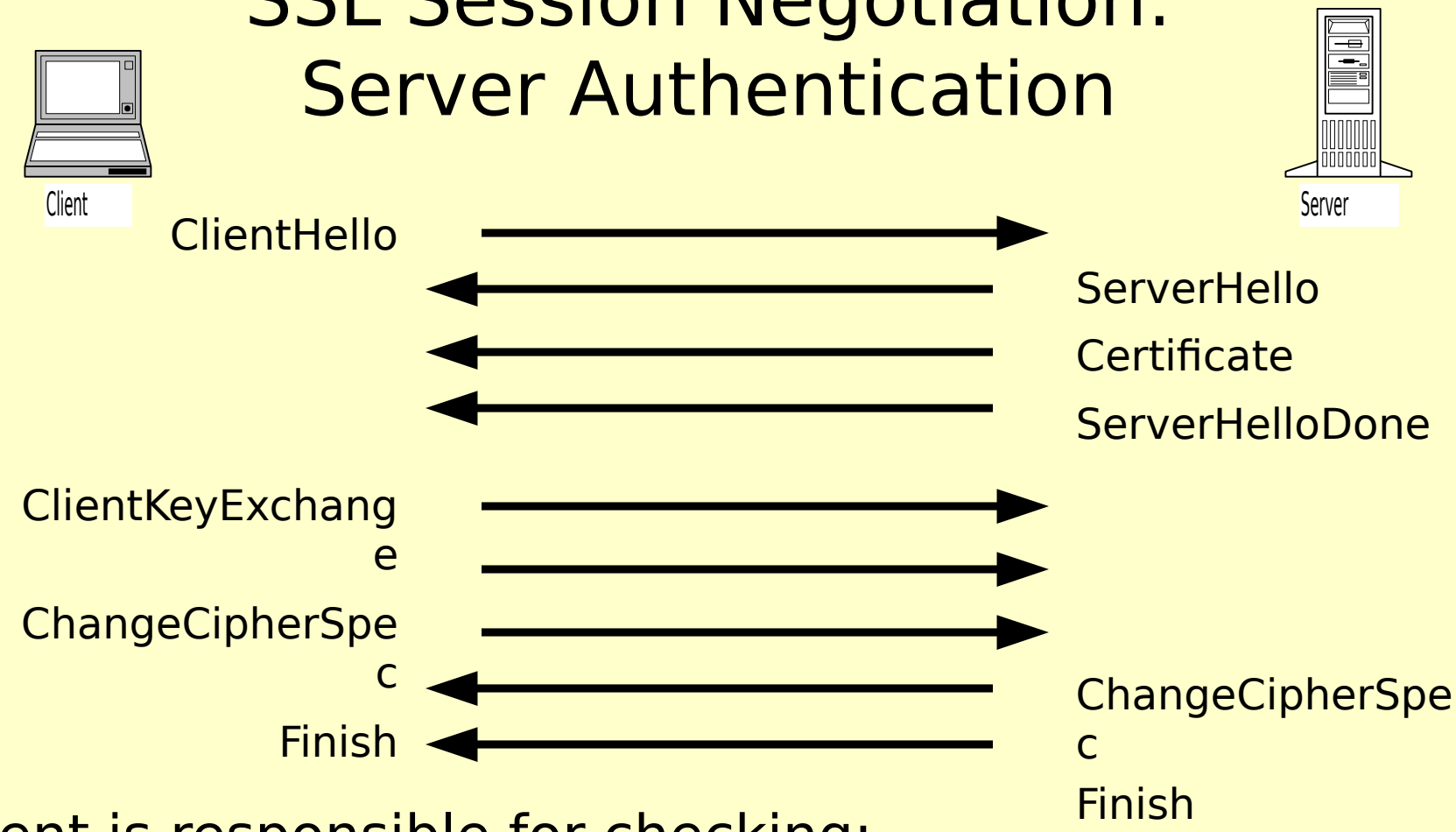
X.509 Certificates: example

Version	3
Serial Number	04:60:00:00:02
Algorithm ID	md5WithRSAEncryption
Issuer (DN)	C=US,O=FooBar, OU=my CA
Period of Validity	**Not Before: Nov 17 00:00:00 2002 GMT** **Not After : Nov 17 00:00:00 2005 GMT**
Subject	C=US,O=MyDomain,CN=www.domain.com
Subject's Public Key	00:e1:73:65:2d:00:77…
Extensions	CA:False
Issuers Signature	51:e4:df:76:c3:97:20:6c…

SSL/TLS


Application Protocol (e.g. http)
ChangeCipher
Alert
Handshake
Record Layer
SSL/TLS
TCP
IP

SSL Session Negotiation: Server Authentication



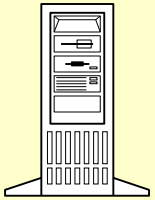
Client is responsible for checking:

- If the Issuer's signature on the certificate is valid
- If the certificate is within the period of validity
- If the Subject (CN) is identical to the server DNS name

Client Certificates

- Basically they are the same as server certificates
- Again, they need to be signed by a trusted third party (the Issuer)
- But, how do we name everyone uniquely?

SSL Session Negotiation: Client and Server Authentication



ClientHello →

← ServerHello

← Certificate

← Certificate Request

← ServerHelloDone

Certificate →

ClientKeyExchange →

→

CertificateVerify →

ChangeCipherSpec →

→

Finish →

← ChangeCipherSpec

← Finish

Certification Authority (CA)

- The CA is the trusted third party
- All certificates are signed with the CA’s private key
  - Including the CA’s signing cert

Courtesy of Netscape...

Edit A Certification Authority - Netscape
This Certificate belongs to:
Secure Server Certification Authority
RSA Data Security, Inc.
US
This Certificate was issued by:
Secure Server Certification Authority
RSA Data Security, Inc.
US
Serial Number: 02:AD:66:7E:4E:45:FE:5E:57:6F:3C:98:19:5E:DD:C0
This Certificate is valid from Wed Nov 09, 1994 to Thu Jan 07, 2010
Certificate Fingerprint:
74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
This Certificate belongs to a Certifying Authority
Accept this Certificate Authority for Certifying network sites
Accept this Certificate Authority for Certifying e-mail users
Accept this Certificate Authority for Certifying software developers
Warn before sending data to sites certified by this authority
OK
Cancel

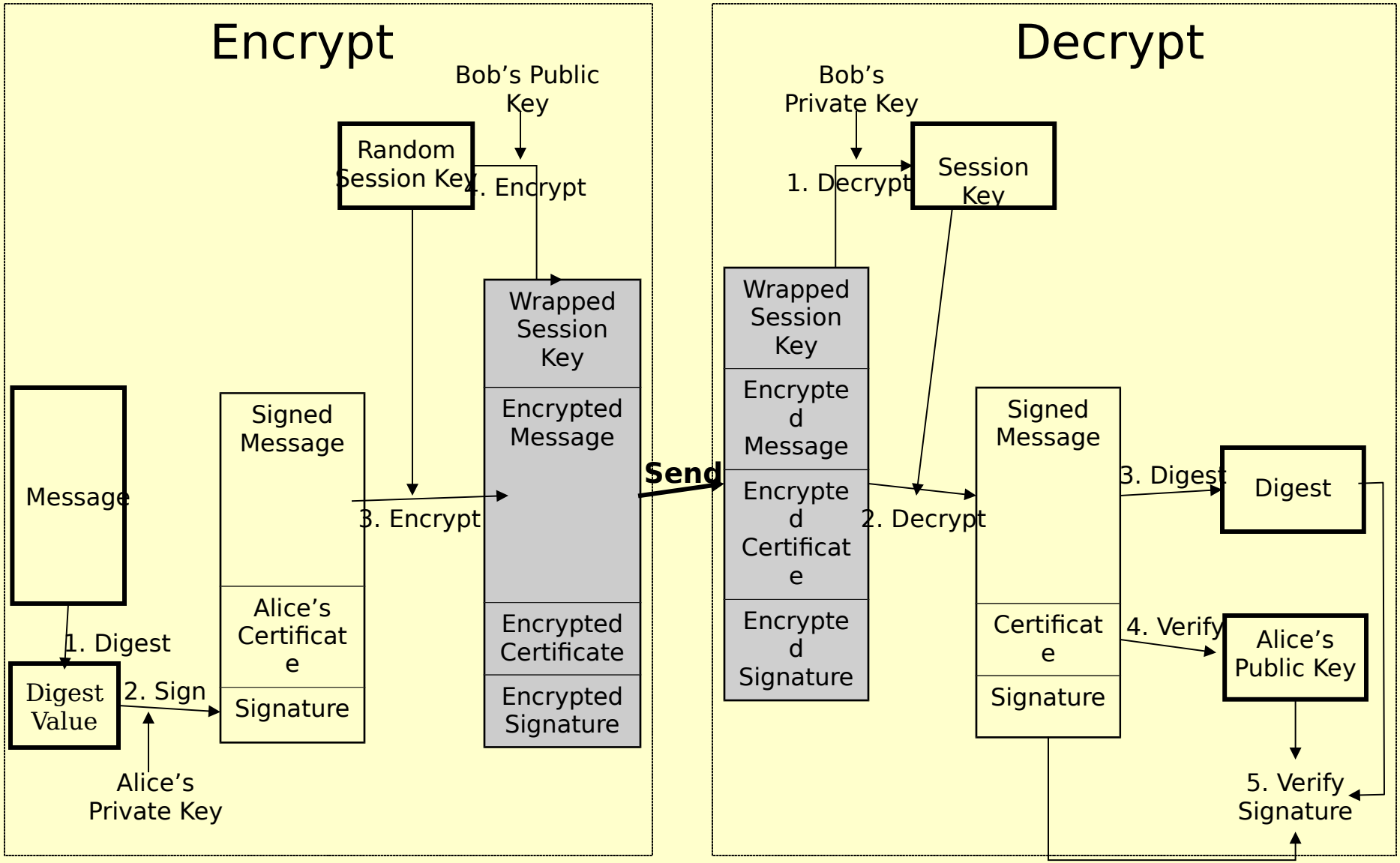
Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Secure E-Mail

- S/MIME
  - X.509 certificate PKI infrastructure
  - Secure extensions to the Multipurpose Internet Mail Extensions (MIME)
  - More prevalent in government and industry
- PGP
  - Free email and encryption system
  - Based off of web of trust
  - Slightly more popular that S/MIME for personal use
  - Basic encryption and signature operation is same as S/MIME

Secure Email



Secure/Multipurpose Internet Mail Extension (S/MIME)

- Security extensions to MIME
  - PKCS#7
  - PKCS#10
- Initially developed by RSA Data Security Inc. in 1995
- To understand S/MIME, must have general understand of MIME

Multipurpose Internet Mail Extension (MIME)

- Basic Simple Mail Transfer Protocol (SMTP) only supports 7 bit ASCII text
- MIME was developed to send binary objects over SMTP
  - Graphics
  - Video
  - Sound
  - Executable files

MIME Types

Type	**Subtype**	**Description**
Image	Jpeg	Image is in JPEG format.
	Gif	Image is in GIF format.
Video	Mpeg	MPEG format
Audio	Basic	Mono 8-bit sound at 8 kHz
Application	PostScript	Adobe Postscript
	Octet-stream	General binary data consisting of bytes.

MIME Transfer Encodings

- MIME can use six different encodings
- The most common is base64 – six bits mapped to a 64 character long table

Security Services Provided by S/MIME

Security Service	**Security Mechanism**
Message authentication	Digital Signature
Integrity	Digital Signature
Nonrepudiation	Digital Signature
Confidentiality	Encryption

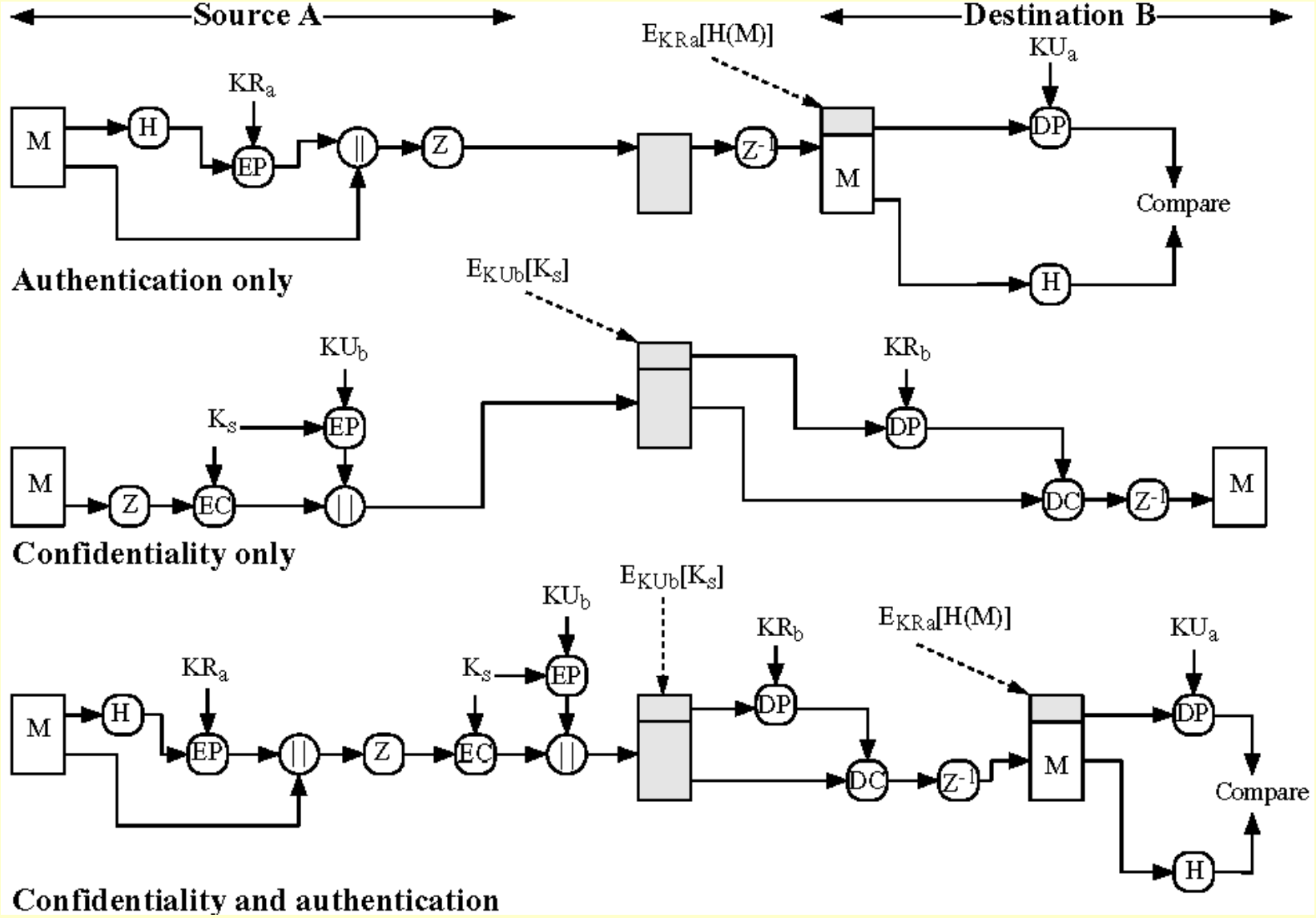
Pretty Good Privacy

- Free secure email that supports most OS’s
- Supports most common encryption algorithms
- Message encryption is performed with symmetric algorithms
- Key distribution is performed with asymmetric algorithms

PGP Services

Function	Algorithms Used	Description
Digital Signature	DSS/SHA RSA/SHA	Hash code is created using SHA-1. The hash is then encrypted using DSS or RSA.
Message Encryption	CAST, IDEA, 3DES, AES or Twofish w/Diffie Hellman or RSA	Message key is CAST, IDEA 3DES, AES or Twofish. Session key is encrypted using Diffie Hellman or RSA.
Compression	Zip	Message may be compressed using zip.

PGP


Source A
Destination B
M
H
KRa
EP
||
Z
Z-1
EKRa[H(M)]
KUa
DP
Compare
Authentication only
EKUb[Ks]
KUb
KRb
Ks
EC
DC
Confidentiality only
Confidentiality and authentication

Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Host Security Devices

- Virus Scanners
- Host Firewalls
- File Modification Detection Software

Network Security Devices

- Virus scanners
- Firewalls
- DMZ
- Intrusion Detection Scanners
- Network Vulnerability Scanners
- VPN devices
- Honeypots
- Backups
- Continuity Of Operations Plan
- Training

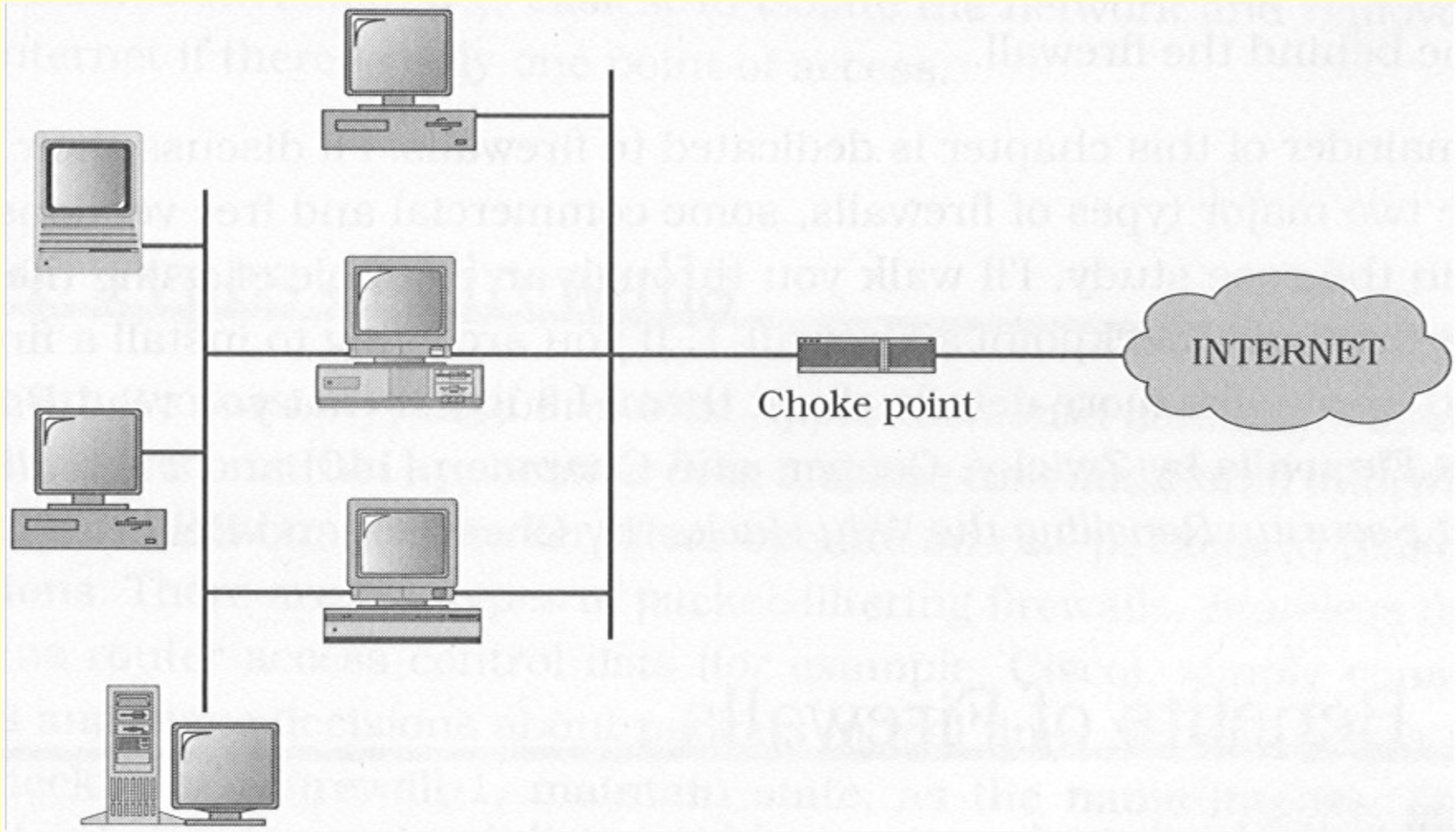
DA Guidance on COTS Security Tools

- Organizations and units who decide to use categories of products that do not yet have Army standards will use the following guidance:
  - GSA schedule
  - FIPS 140-1 compliant
  - Have performed satisfactorily in the past per the FAR
  - Evaluated/used by an authoritative source
  - Certification stating the software code shall be free of vendor/engineer created front/backdoors
  - Coordinate with supporting CERT
  - Meet COE and JTA minimum requirements

Firewalls

- Combination of hardware and software used to make access control decision about traffic on a network in order to enforce a uniform policy at the point connecting the network to other networks
- IPSec/VPNs frequently incorporated with firewalls
- Firewalls must be at a chokepoint

Firewall Chokepoint



Firewall Types (1 of 2)

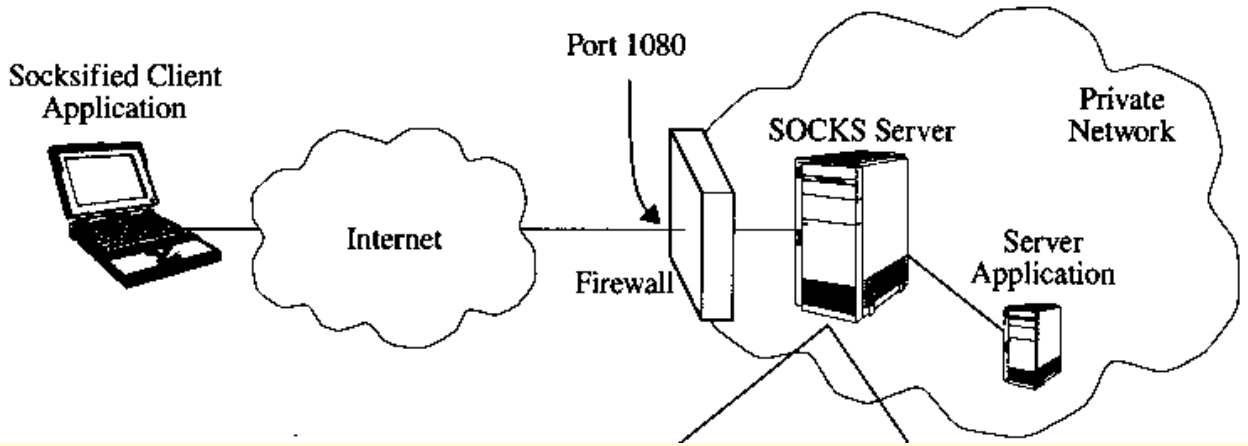
- Packet Filtering
  - **Stateless Firewall**
    - Routers with Access Control Lists (ACL)
    - Makes decisions based on any or all of the following
      - Source IP address
      - Destination IP address
      - TCP or UDP port numbers
      - ICMP header
      - Packet size
      - Application data
  - **Stateful Firewall** – also called circuit-level gateway
    - Many commercial firewall applications are packet, stateful firewalls
    - Track TCP flags – i.e. SYN, SYN-ACK, and ACK
    - Perform faster that Application-Level or proxies

Firewall Types (2 of 2)

- Application-Level Gateway
  - Also know as proxies
  - Reconstruct application data
  - Understands application data
  - Decisions can be made at a much finer granularity – more accurate that stateful firewalls for supported protocols
  - Need a proxy for every application protocol
  - Not transparent – clients must be configured
  - Example is SOCKS

SOCKS

- Proxy protocol for client applications
- SOCKS Server provides the following
  - Authenticates client
  - Controls access to server
  - Creates a proxy circuit
  - Relays data between client and server
  - Log access requests and traffic
- Provides no confidentiality
- Requires “socksified” client and increases latency



Firewalls

- Mandatory in unclassified and SBU environments
- Recommended but not mandatory for Secret and above
- Normal military usage allows unrestricted outbound access

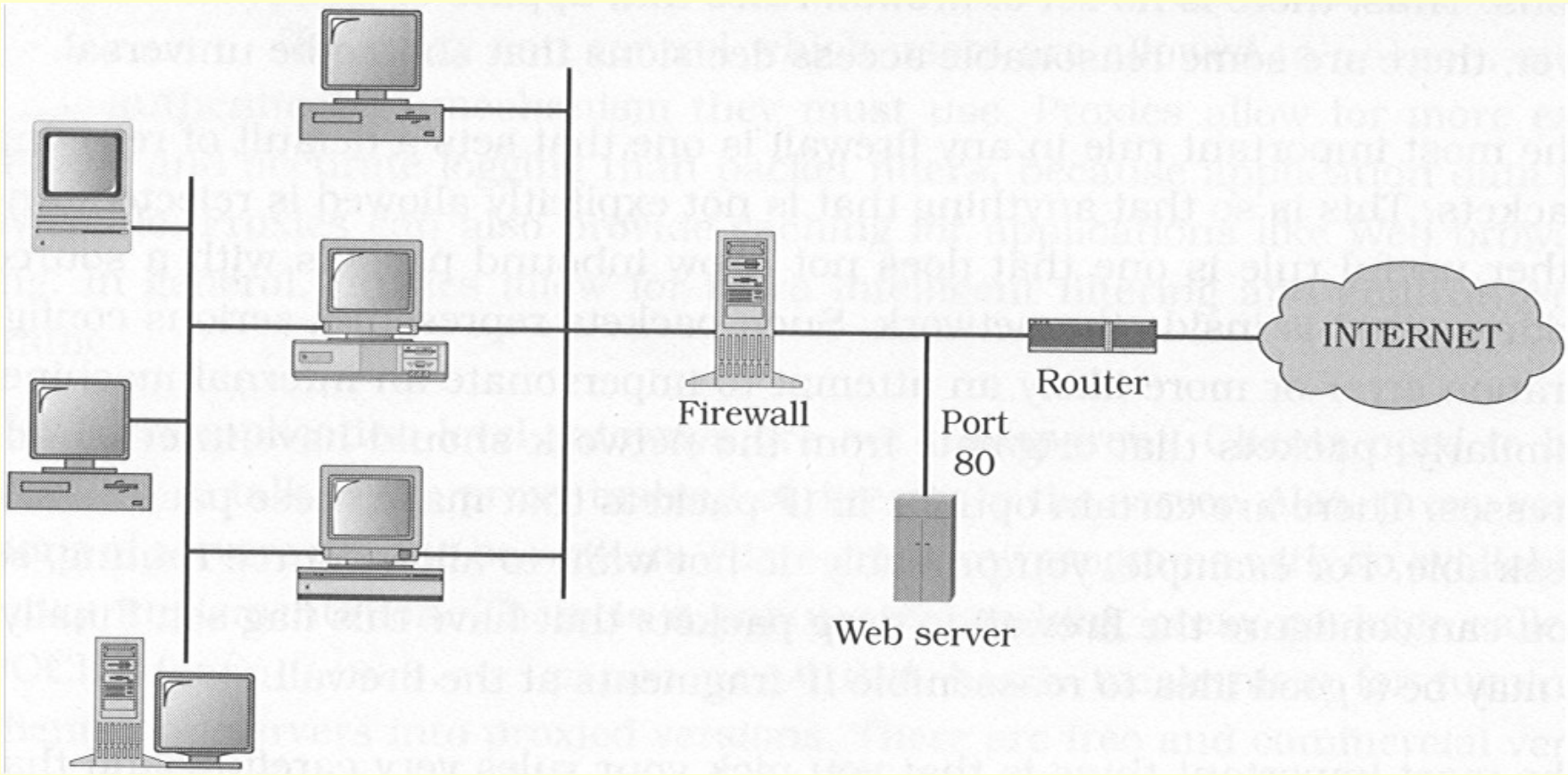
Firewalls out there

- Gauntlet -- Network Associates – both stateful and proxy
- Lucent Managed Firewall – Lucent – stateful
- PIX – Cisco – stateful but support proxy for certain protocols (HTTP and SMTP)
- Raptor – Symantec -- proxy
- Sidewinder -- Secure Computing Systems -- proxy
- Sunscreen – Sun -- stateful
- Firewall-1, Checkpoint – stateful
- Most newer enterprise firewalls are not hybrids
  - Support both stateful and application proxies
  - Most hybrids only due application proxies for certain protocols (HTTP)
  - Gauntlet uses application proxy for the first few packets and then switches to stateful

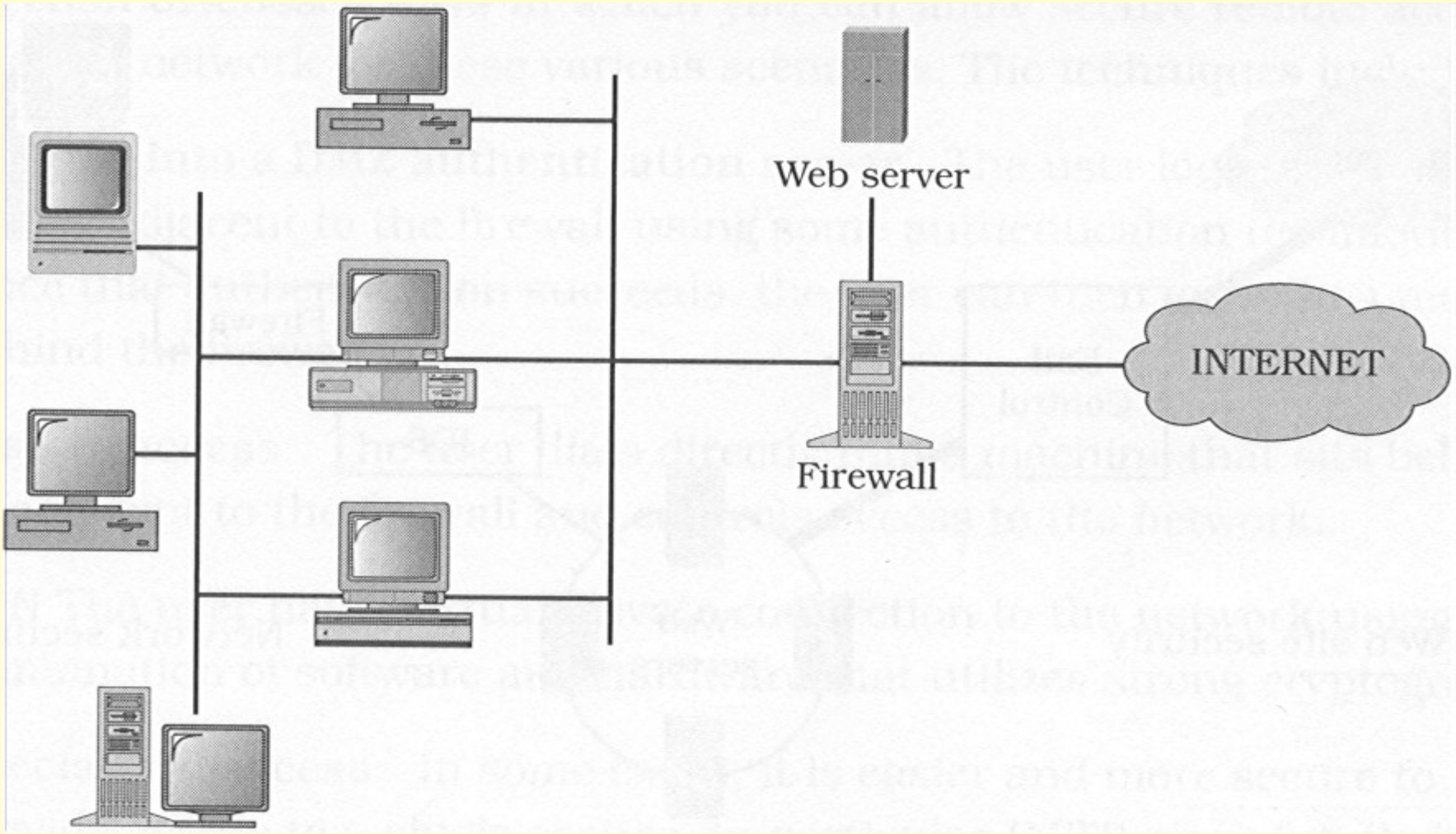
DMZ

- Area between protected network and unsecure internet where servers are placed
  - Area between two firewalls
  - More protected than internet
  - Not as protected as inner network

DMZ



DMZ



Intrusion Detection Systems

- Refers to software tools that attempt to identify malicious network traffic
- Detects unauthorized activity by patterns/signatures
- Operation is analogous to a combination of a packet sniffer and virus scanners
- Current IDS's have high false alarm rate -- called false positive
- Looks for
  - Multiple SYN packets
  - Irregular ICMP traffic
  - Signatures of DDOS tools
- Requires well trained analyst
  - Isolate attacks from false positives
  - Modify rule sets
  - Knowledge of network
  - Detailed knowledge of all TCP/IP protocols

Intrusion Detection Systems

- RealSecure -- Internet Security Systems
  - Network based
- Cybercop Monitor -- Network Associates
  - Host based
- Intruder Alert -- Symantec
  - Host based
- Snort

Network Vulnerability Scanners

- Scans the entire network or one computer and provides a definitive understanding of all available devices and services
- Renders a road map of potential exposures
- Tests for common software defaults – buffer overflows
- Tests susceptibility to DoS attacks

Network Vulnerability Scanners

- Cybercop Scanner -- Network Associates
- ISS Scanner -- Internet Security Systems
- Security Test and Analysis Tool (STAT) -- Harris Corporation
- Nessus
  - Free
  - Linux based
  - Rated better than the previous three

Securing Network Layers

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design

Honeypot

- An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system
- Honeypot purposes
  - Learning where weaknesses are
  - Hacker can be caught and stopped before hacking into something important
  - Can create more secure systems that are potentially invulnerable to future hackers

Backups

- One of the most important forms of network security
- Allow networks and servers to recover not only from break-in/hacks but also other natural disasters
- Backups are an often overlooked part of network security in the military
- Extremely important not only to do backups but to test your backups periodically

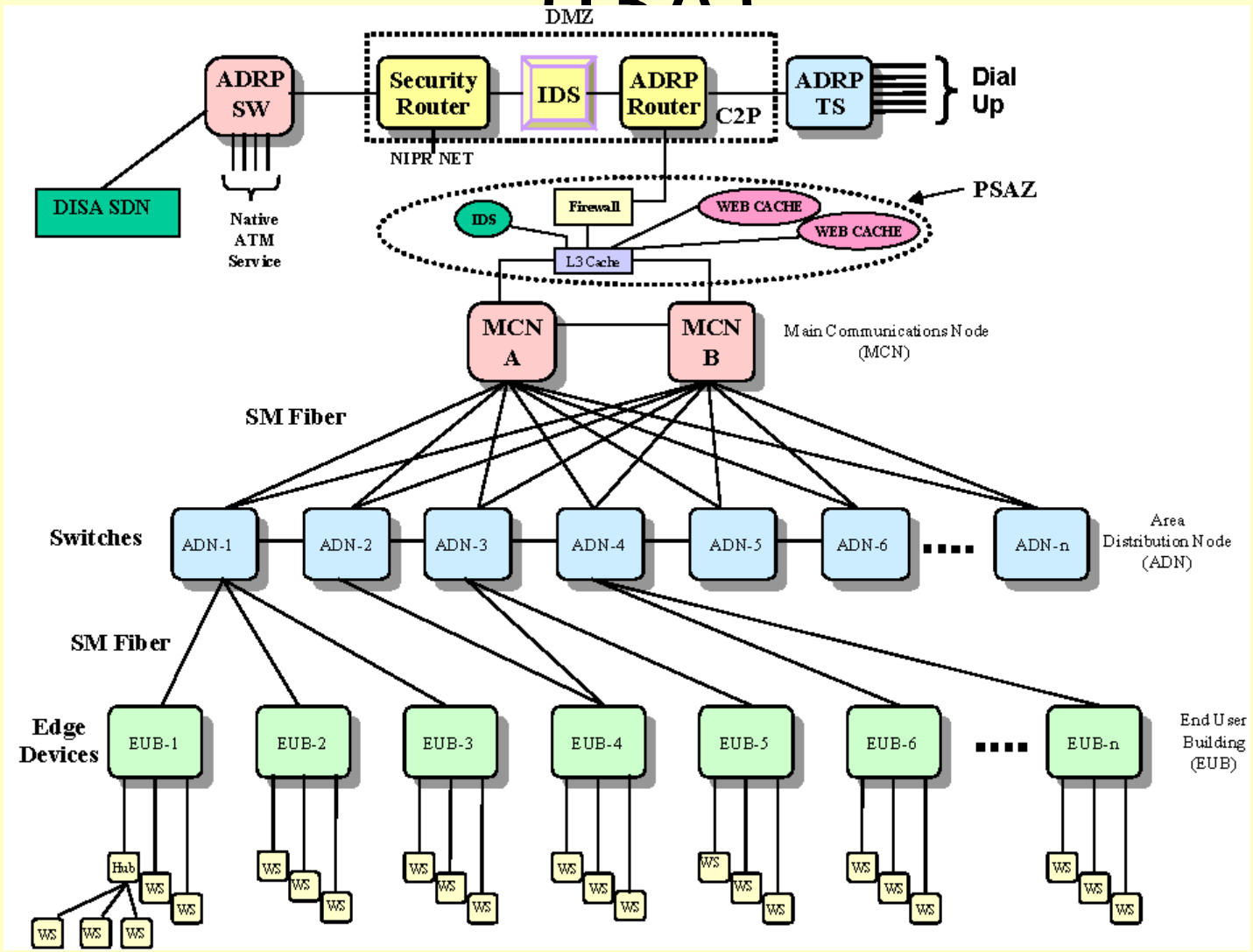
Continuity Of Operation Plan (COOP)

- Refers to a detailed plan in case primary server site is destroyed or damaged by man-made or natural disasters
- All critical networks should have a COOP plan
- Need to have a backup server site
  - Hot
  - Warm
  - Cold
  - Shared

Installation Information Infrastructure Architecture (I3A)

- DISC4’s plan to upgrade the CONUS base telecommunication infrastructure
- Includes fiber and networking components
- Establishes an Army-wide IT architectural design standard that supports Army installation IT modernization.
- I3A does not identify requirements and/or dictate solutions.

Installation Information Infrastructure Architecture (I3A)



Defense in Depth

ISEC's Approach to

"Defense in Depth"

Level 1 Security - Perimeter (WAN Interface)

High Level Packet Filtering of Commonly Understood Vulnerabilities

- -Ping
- -Source Routing
- -Internal Source Address
- -Bad Boy List

Level 2 Security - Backbone (Installation Infrastructure)

Installation Level Policy Enforcement and Session State Awareness

- -Deny Un-established Connections
- -Drop packets not associated with session

Level 3 Security - Enclave (Organization/Office)

Organization Level Policy Enforcement

- -Specific to Organization
- -Definable and Enforceable
- -May include service Proxies
- -Email Server Anti-Virus/Malicious Code Detection

Level 4 Security - System /Host (OS & Application)

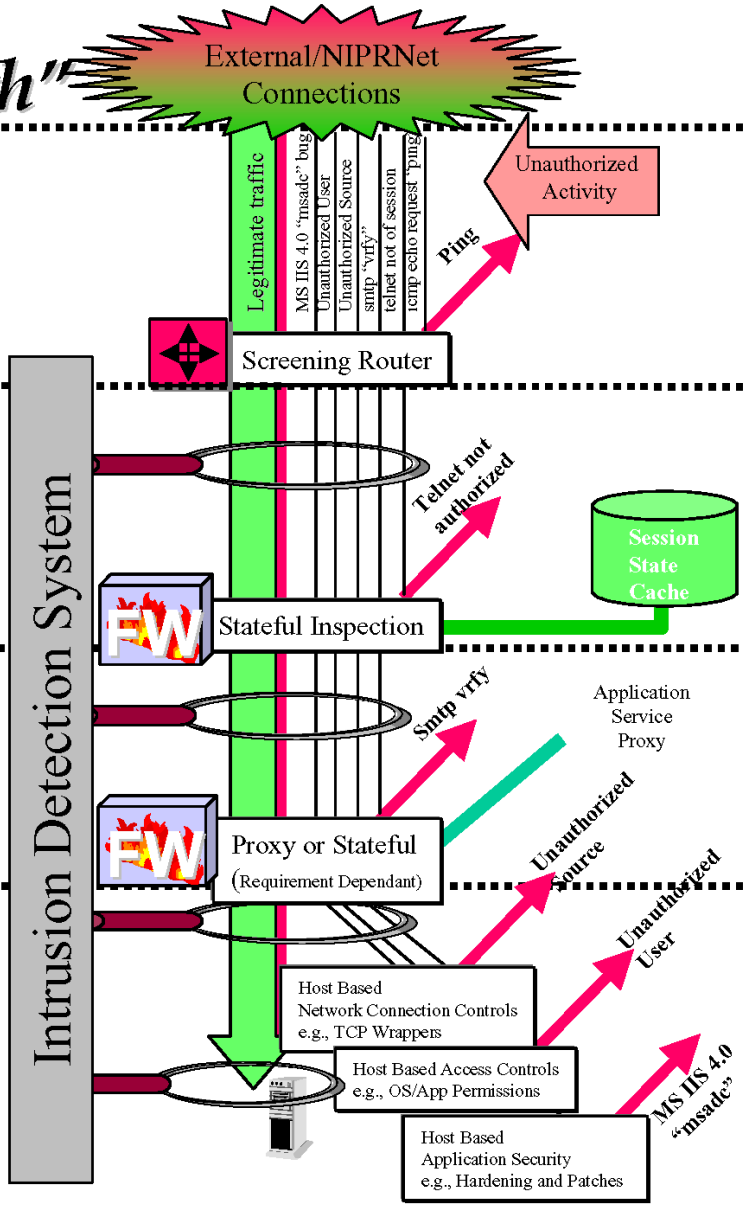
Information System Specific Policy Enforcement

- -Operating Systems Hardening
- -Network Connection Acceptance (TCP Wrapper)
- -User ID and Authentication
- -Application Security

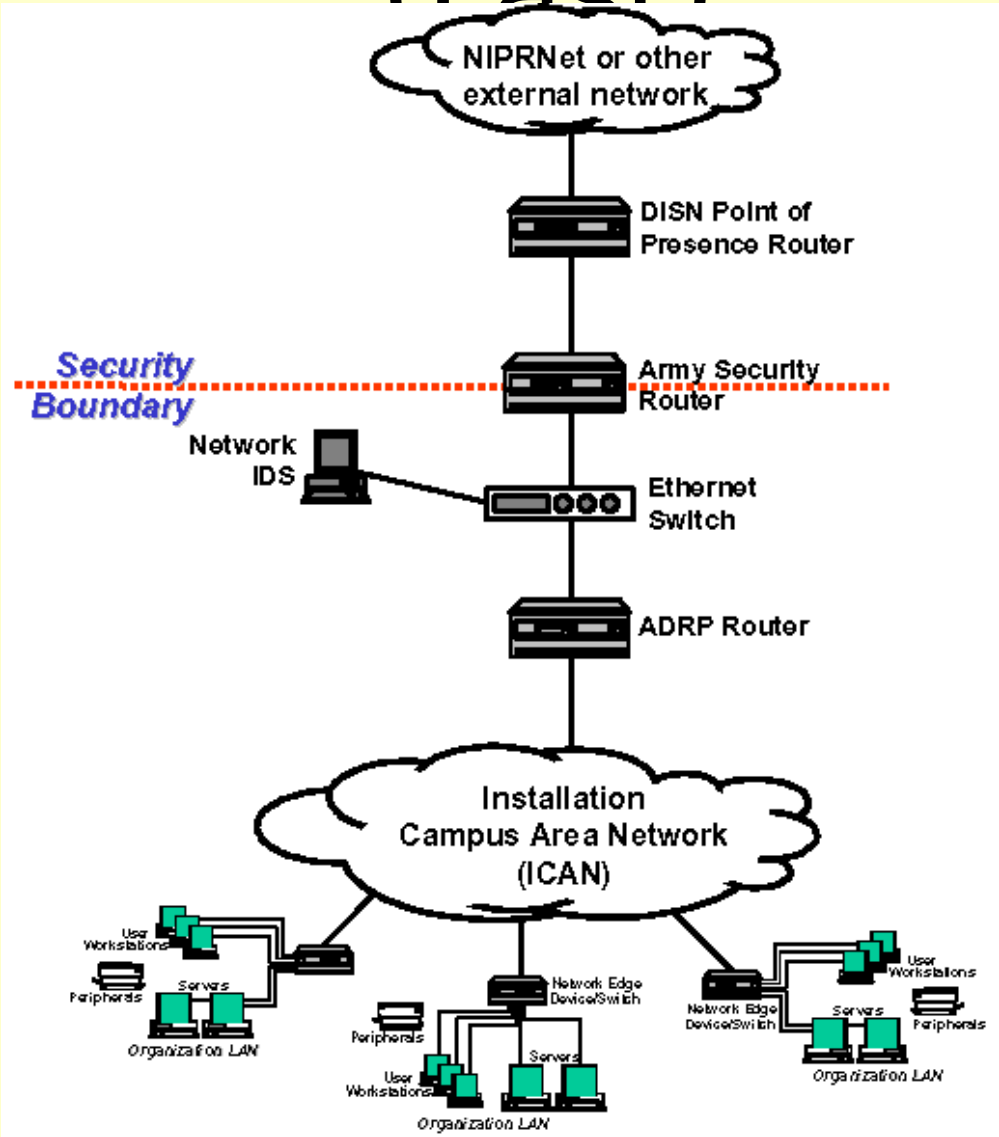
System Vulnerability Assessment and Correction

Password control

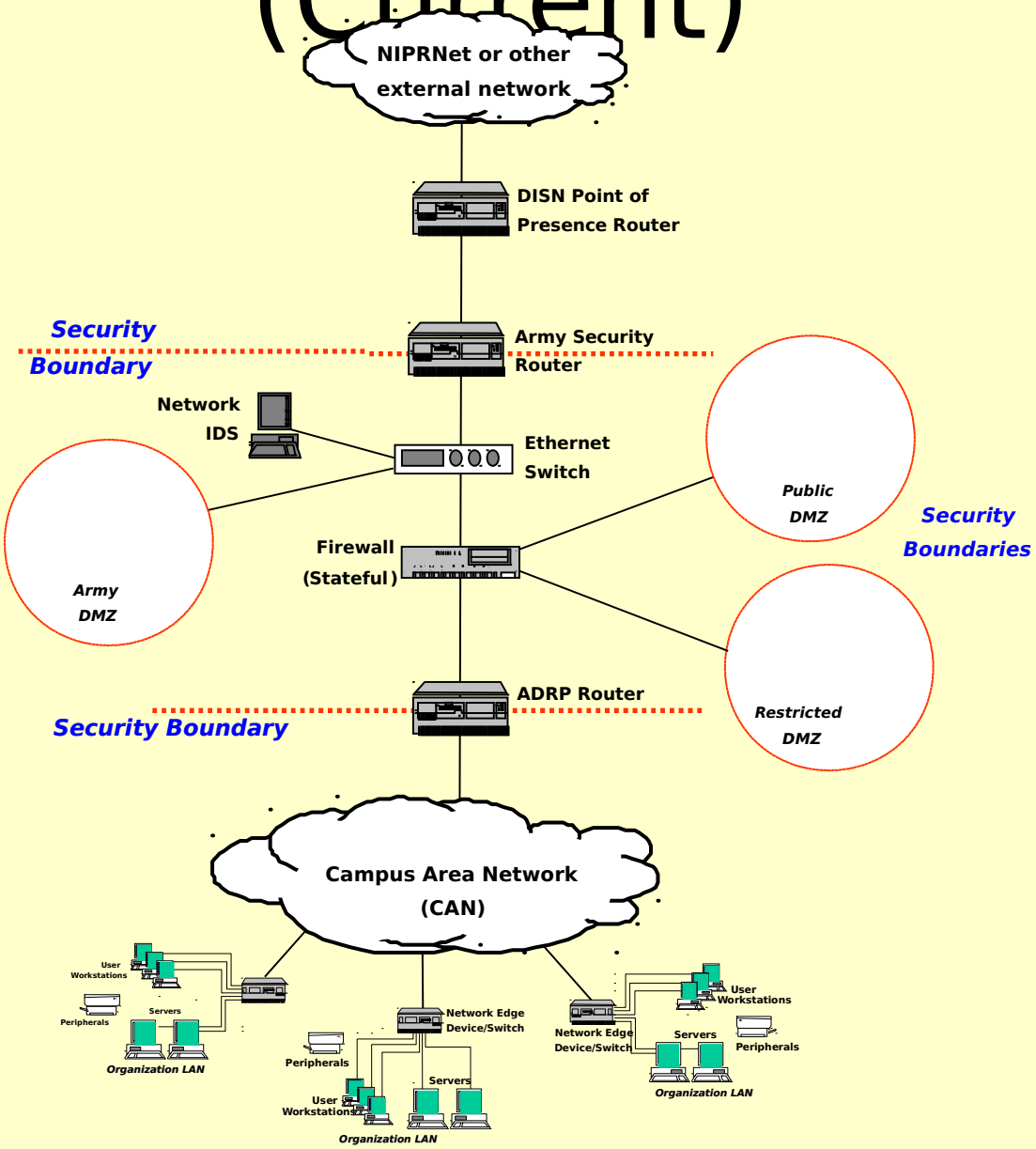
Anti-Virus



Top Level Architecture (Past)



Top Level Architecture (Current)



Summary

- Review TCP/IP
- Virtual Private Network (VPN)
- Layer 2 VPNs
- Layer 3 VPNs -- IPSec
- Secure Upper Layer Transport Protocols (Host to Host)
- Secure Electronic Mail
- Host and Network Security Devices
- Unclassified Network Security Design